

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: MS: AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on December 5, 2005

Scott W. Kelley December 5, 2005
Scott W. Kelley, Reg. No. 30,762 Date



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|-------------------------------|---|-------------------------------|
| In re Application of |) | Group Art Unit: 2876 |
| |) | |
| Mark M. Kotik, et al. |) | Examiner: Nguyen, Kimberly D. |
| |) | |
| Serial No. 10/712,935 |) | |
| |) | |
| Filed: November 12, 2003 |) | Docket No. PREDYN-44227 |
| |) | |
| For: IDENTIFICATION BAND WITH |) | |
| ADHESIVELY ATTACHED |) | |
| COUPLING ELEMENTS |) | |
| |) | |

SUPPLEMENTAL DECLARATION OF Walter W. Mosher, Jr.
UNDER 37 CFR 1.131

WALTER W. MOSHER, JR. hereby declares as follows:

1. I am one of two co-inventors of the subject matter of the above-identified U.S. Patent Application Serial No. 10/712,935, filed Nov 12, 2003.
2. I am a founder and Chief Technical Officer of Precision Dynamics Corporation (hereinafter referred to as PDC). PDC is the assignee of the above-identified application.
3. I have worked in the field of identification devices for more than 45 years and RFID technology for over 15 years. For example, I am one of the joint inventors of Charles, et al., U.S. Patent No. 4,318,234 (issued March 9, 1982, filed January 10, 1977), which relates to an identification device with versatile imprinting means. I am also the sole inventor of Mosher, Jr., U.S. Patent No. 5,937,600 (issued October 26, 1999, filed September 9, 1998), which relates to a laminated radio frequency identification device. I am also a

joint or sole inventor of the numerous other U.S. Patents relating to RFID identification devices.

4. Under my direction, PDC (assignee of the present application) has actively engaged in a research and development program related to radio frequency identification (RFID) with the aim of creating innovative technologies, RFID products based upon these technologies, and manufacturing support to produce these products.

5. PDC has engaged numerous consultants and assembled an in-house development team, including co-inventor Mark Kotik. The personnel have changed over the years, but the aims of the program and my direction have remained constant.

6. As shown in the prior declaration I, along with my RFID development team, conceived of the subject matter of the present application and its parent application prior to November 13, 2001, the date the De La Hueraga application, U.S. Publication No. US2002/0084904 was filed with the United States Patent and Trademark Office.

7. From that date forward, including the time period from October 1999 to and beyond March 18, 2002, PDC diligently worked at reducing the subject matter of the present application to practice. This work is documented in three parallel fields of activity all linked to the responsibility of developing RFID technologies and products: consultant work; in-house organization and RFID projects; interaction between consultant and in-house activities.

8. My review of correspondence, reports, drawings, and other materials documenting our conception and reduction to practice of the enhanced identification wristband invention indicates, and documents confirm, that this conception occurred well prior to the filing date of the De La Huerga application and reduction to practice continued up to and beyond the March 18, 2002 filing date. See Exhibits A through P, attached hereto.

9. Scott Balzer, an in-house RFID engineer and member of my RFID development team, worked on various RFID projects related to the reduction to practice of the present application. Excerpts from an October 11, 1999 laboratory notebook maintained by Mr. Balzer are submitted as **Exhibit A**. A December 1999 excerpt from Mr. Balzer's notebook demonstrates his continuing work in this area and documents his communications with Michael Beigel, a consultant with PDC, and others regarding the pricing and purchase of a reader module, an antenna and connectors related to RFID. A June 9, 2000 excerpt from Mr. Balzer's notebook further documents Mr. Balzer's continuing work in RFID development. This page reflects a meeting regarding RFID projects discussing materials and compounds for bands and sealants.

10. An October 31, 1999 report from Mr. Balzer documenting the status of active RFID engineering projects is submitted as **Exhibit B**. The report indicates the scope of activities required for Mr. Balzer on the project, designated as "88-99-01 RFID: Start – 01/01/99 Finish – 12/31/01". In

addition to providing a clear indication of the on-going, long-term nature of my RFID team's research and development, this report details how a purchase demonstration using RFID wristbands has been completed and an access control demonstration is in process. Various modifications for the access control demo are documented. The report also documents efforts to place an RFID wristband system into a major hospital for testing.

11. A February 20, 2000, memorandum from Dr. Yang Yang, a consultant for PDC and another member of my development team, is submitted as **Exhibit C**. This memo is "an assessment of the flexible RFIDs" containing non-silicon components and processable by printing techniques - both key elements of the present application. The memo discusses components required in an RFID tag circuit. The memo concludes with reference to "demonstrat(ing) a workable RFID containing polymer electronic components". Dr. Yang works on several RFID-related projects for PDC including the evolving field of organic RFID, another key element of the present application.

12. A March 3, 2000 report from Mr. Beigel regarding Circuits for Flexible RFID Tags is submitted as **Exhibit D**. This report was revised on April 17, 2000. The report details specifications and circuit diagrams for RFID tags that could be fabricated directly on flexible substrates using organic or other thin film semiconductor devices. Several schematic drawings that contributed to the theory underlying the present application were included in

the report.

13. An Engineering Organizational Chart of Research Engineering dated March 20, 2000 is submitted as **Exhibit E**. This chart indicates the organization of consultants and in-house engineers working on the various RFID projects, including the present application. Sam Chaoui, at that time the research engineering manager, reported to me and to Oswaldo Penuela. At the time of the work on the present invention, Mr. Penuela was Vice President of Operations and Engineering and directly involved in in-house RFID development.

14. A June 2, 2000 report prepared by Mr. Beigel is submitted as **Exhibit F**. This report concerns Proposed Year 2000 Project Activities, including the Polymer RFID Project. The report was revised on June 20, 2000. The report details research efforts regarding emerging technologies related to polymer and flexible electronics. On page 3, the report discusses printable and polymer diodes, as well as, a demonstration of RFID tags on flexible substrates.

15. A June 5, 2000 memorandum prepared by me is submitted as **Exhibit G**. This memo is a follow-up on RFID Status Meeting Action Items. This memo discusses various ideas/concepts related to the RFID project, including: methods of inlet installation via lamination and encapsulation; inserting inlets into Superband and heat sealing end as encapsulation method; a conductive band for tamper detection; a co-extruded fiber optic

within the band material for conductivity; an RFID inlet integrated within an adhesive, heat laminating label; laminating an inlet within a Compuband or Superband (specific band media in the PDC product line); and printing conductive ink antennas on band along with polymeric chip. Specifically, the item dealing with "Conductive band for tampering detection" relates to the present application.

16. A February 14, 2001 memorandum from Sam Chaoui is submitted as **Exhibit H**. This memo concerns the scheduling of regular meetings to discuss the ongoing, regular development of all elements of the present application under my leadership.

17. An April 18, 2001 memorandum from Sam Chaoui to various individuals, including me and Mr. Penuela, is submitted as **Exhibit I**. The memo concerns RFID Project Management, confirmed PDC's emphasis on RFID work, and discussed the need for a full-time RFID project manager "[d]ue to the ever-increasing workload that the existing project management is facing," indicative of the ongoing development of the present application.

18. A May 2, 2001 report prepared by Mr. Beigel is submitted as **Exhibit J**. This report concerns ISO/IEC Standards Pertaining to the RFID Project and details research into national and international standards applicable to PDC's RFID projects, including the present application.

19. A June 13, 2001 draft patent application titled Wristband Patch Antenna is submitted as **Exhibit K** and documents the work of consultant

John Tuttle. Such structure was in the original draft of the present application but later separated out. Other elements of Mr. Tuttle's work were also separated out from the present application just prior to its filing and filed as a separate application on March 5, 2002 (now US Patent No. 6,888,502 Microstrip Antenna for an ID Appliance).

20. A September 17, 2001 e-mail and report from Mr. Beigel to me and Mr. Penuela, among others, is submitted as **Exhibit L**. This e-mail documents revisions to a section of a report from a September 10, 2001 meeting regarding the RFID project. This e-mail and underlying report relate back to invention ideas discussed in November 1996. This report clearly relates back to the conception of the RFID project in 1996 and references the ongoing development work performed by consultant Beigel and the PDC staff under my direction.

21. An October 16, 2001 report prepared by Mr. Beigel on the RFID Project – Project Priorities is submitted as **Exhibit M**. This report was revised on October 31, 2001. This report list several elements (printable RFID in flexible substrate, secure RFID wristband, patch antenna wristband, RFID with flexible battery, RFID standards, organic semiconductor projects, high frequency RFID, wristband RFID antenna activated by closure of wristband, and conductive adhesives activating RFID tags) that became part of the present application, both as it currently stands and as it was originally filed before being subject to restriction.

22. A November 6, 2001 draft application prepared by Clark Bell, a consultant, entitled "Secure Radio Frequency Identification Wristband" is submitted as **Exhibit N**. This application deals with security and "tamperproof" qualities of RFID wristbands, key elements of the present application.

23. A November 30, 2001 report prepared by Mr. Beigel on an Enhanced Electronic ID Wristband is submitted as **Exhibit O**. This report was revised on December 12, 2001. This report is suggested as containing material that may be added to the "Secure RFID Wristband" application. The transmitting e-mail mentions that the report "contains the unifying architecture to bring together aspects of the other disclosures [PDC has] been working on." This report links all of the previous work – dating back to 1996 – to the present application as originally filed. Page 1 of the report lists names of the various co-inventors and possible co-inventors on this and other applications resulting from this massive research and development project.

24. A March 7, 2002 e-mail and draft application for an Enhanced Identification Band (aka "The MONSTER patent application") with accompanying drawings is submitted as **Exhibit P**. This application was revised into the filed form of the parent of the present application after separating out elements of earlier drafts into a parallel application that ultimately became US Patent No. 6,888,502 "Microstrip Antenna for an ID Device," filed March 5, 2002. This e-mail shows representative drawings that

remain part of the present application and its divisional application.

25. Co-inventor Mark Kotik was hired by PDC in September 2002. As such, there are no documents between October 1999 and March 2002 that bear Mr. Kotik's name or were produced by Mr. Kotik in relation to the RFID development. Subsequent to that, upon joining PDC's in-house development team, Mr. Kotik performed some critical development work on the present application after the parent application was filed in March 2002.

26. It should be clear from the attached exhibits that the cited subject matter of De La Huerca was well-known to the inventors of the instant application, as we had conceived of and been reducing to practice this subject matter well prior to the De La Huerca filing date.

I further declare that: all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such false statements may jeopardize the validity of the application or any patent resulting therefrom.

Date: November 30, 2005



Walter W. Mosher, Jr.

Attachments

Exhibit A – October 11, 1999 Laboratory Notebook excerpts (3 pages)

Exhibit B – October 31, 1999 Status Report (1 page)

Exhibit C – February 20, 2000 Memo (1 page)

Exhibit D – March 3, 2000 Report (13 pages)
Exhibit E – March 20, 2000 Organizational Chart (3 pages)
Exhibit F – June 2, 2000 Report (5 pages)
Exhibit G – June 5, 2000 Memo (1 page)
Exhibit H – February 14, 2001 Memo (1 page)
Exhibit I – April 18, 2001 Memo (1 page)
Exhibit J – May 2, 2001 Report (3 pages)
Exhibit K – June 12, 2001 draft application (16 pages)
Exhibit L – September 17, 2001 Report (9 pages)
Exhibit M – October 16, 2001 Report (12 pages)
Exhibit N – November 6, 2001 draft application (14 pages)
Exhibit O – November 30, 2001 Report (10 pages)
Exhibit P – March 7, 2002 E-mail and drawings (97 pages)

LABORATORY NOTEBOOK

Notebook No.: 1008

Assigned to: SCOTT BALZER

Date: 10-11-99


Use Nalge Cat. No.

6301-1000
to reorder.

Copyright 1973, Nalge Company
Printed in U.S.A.




~~CATHY~~ HODGSON (831) 438-7000 Ext. 213

 **ESCORT MEMORY SYSTEMS**
A DATALOGIC GROUP COMPANY

MARK NICHOLSON
President/CEO

Tel: (831) 438-7000 Ext. 219
Toll Free: (800) 826-3893
Fax: (831) 438-3768
Pager: (888) 907-2163
Cellular: (831) 529-1964
E-Mail: mark_nicholson@ems-rfid.com

Corporate Office
3 Victor Square
Scotts Valley, CA 95066 USA
http://www.ems-rfid.com

 **ESCORT MEMORY SYSTEMS**
A DATALOGIC GROUP COMPANY

Steve Peters
EMS Regional Sales Engineer

2085 Courage Street
Vista, CA 92083
www.ems-rfid.com

Office/Cel/Pgr: 909/288-7988
Fax: 760/598-0804
E-Mail: speters@ems-rfid.com

Get Sm needed

Irwin Thall
Western Sales Manager - RFID

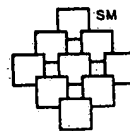
Checkpoint

www.checkpointsystems.com

Checkpoint Systems, Inc.
101 Wolf Drive, P.O. Box 188
Therofare, New Jersey 08086
856-848-1800
1-800-257-5540, Ext. 3400
Voicemail: 3841

1737 Wellesley Drive
Thousand Oaks, CA 91360
(805) 374-8963
FAX: (805) 374-2084

**BEIGEL
TECHNOLOGY
CORPORATION**



Michael L. Beigel
President

Holidays! MB
Happy

PHONE: (760) 633-3868
FAX: (760) 633-3819
E-MAIL: beigel@beitec.com
www.beitec.com

308 VIA JULITA • ENCINITAS, CA 92024 • U.S.A.

from Steve Peters EMS for long range read
Reader module is \$2,950.00 handles up to
6 antennas (time multiplexed)

+ 5ft antenna is \$1,395.00

+ connectors \$200.00

4,545.00

- 20% if business partners

\$3,636.00

Continued on Page

Read and Understood By

Signed

Date

Signed

Date

POW MEETING 6/9/00 PRSPT
 190 SERIES VINYL BAND FOR POSSIBLE FOR TAG

- VINYL BAND WILL NOT BE MADE FOR TAG TI-TAG-IT MUST.
- FOR CONSIDERATION AS A POSSIBLE SOLUTION IS A SPECIAL COATING OR ADH SEALING TWICE.

MEETING WITH ROD KATZER

14 or 15K for market evaluation possible.

(908) 879-4973

Target in July

PARALOC@Yahoo.com

- Terms 5% upfront, 5% on final

JAY PRONILIMB

1MO, EXHIBITOR

WWW.PRONILIMB.COM

(7800) 920-3555

Continued on Page

Read and Understood By

Signed

Date

Signed

Date

STATUS REPORT OF ACTIVE ENGINEERING PROJECTS

Week Ending:

Engineer Scott Balzer
Dept: RFID
Dept# 88

| PRIORITY | PROJECT NO. TITLE | START DATE FINISH DATE | WEEKLY ACTIVITY | STATUS |
|----------|----------------------|---------------------------|---|--|
| A1 | 88-99-01 RFID | 01/01/99 12/31/01 | Completed the software and installed the RFID Wristband Coffee purchase demo. system. Started new software for the access control demo. system, utilizing the new EMS reader electronics and our improved gate antenna. Received and currently evaluating proposal from Jim Potter (eXXisoft) for POS and Access control software. Arranged a meeting with Escort Memory Systems for developing a custom gate antenna per PDC specs. and got updates from E-CODE and eID Solutions. | Coffee demo. system 100% complete. Access control demo. system 75% complete. Gate antenna modified into 3D system, but sensitivity stills needs to be improved. E-CODE is almost ready with some prototype passive RFID tags. Information is slow coming, but will keep after them. Alex Gelbman (eID Solutions) is in the final proposal stage, competing with only one other company for selling an RFID wristband system into a major hospital. The other company is selling a barcode wristband system. Delivered RFID System implementation scenarios to Tom Mahoney and waiting for Response and 60% completed on the I-CODE Product Schedule. |
| A2 | 88-99-02 PDF-417 | 09/13/99 12/31/01 | No Activity | |

10/31/1999

Yang Yang
13730 Bayliss Road
Los Angeles, CA 90049

~~2-21-00~~

1

To: Mr. Walter Mosher

From: Yang Yang

Subject: Flexible RFID

Date: February 20, 2000

C.C.: Mr. Ozzie Penuela, Mr. Tom Mahoney, and Mr. Michael Beigel

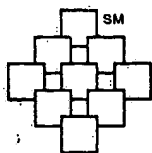
Per request by Mr. Penuela, this document serves as an assessment to the flexible RFIDs, which contain non-silicon components and can be processed by simple printing technique. Particular concerns are the availability on non-silicon and printable electronic components. This memo emphasizes on the research level of these components, potentially to be operated at either 125KHz or 13.5MHz.

As indicated at Mr. Beigel's memo (Beigel's list), RFID tag circuit requires the following components:

1. Inductor antenna;
2. Resonance capacitor;
3. DC Power extractor;
4. Loading element;
5. Timer or counter;
6. Logic gates;
7. Data memory elements;
8. Interconnect wires, vias, and bridges.

(Please note, in this memo electronic components represent the above items. Electronic elements mean the basic electronic parts such as diodes, transistors, resistors, and capacitors.)

Currently, the on-going UCLA-PDC project is focusing on producing polymer diodes for the power supply of a RFID. We have also demonstrated the feasibility of polymer capacitor to be used in the same power supply. The goal of that work was to demonstrate a workable RFID containing polymer electronic components in order to satisfy the requirement of filing a useful patent with enabling disclosure.



**BEIGEL
TECHNOLOGY
CORPORATION**

www.beitec.com

• PHONE: (760) 633-3868
• FAX: (760) 633-3819
• E-MAIL: beigel@beitec.com

308 VIA JULITA • ENCINITAS, CA 92024

PRECISION DYNAMICS CORPORATION

POLYMER RFID PROJECT

CIRCUITS FOR FLEXIBLE RFID TAGS

ALL PAGES CONFIDENTIAL MATERIAL

Prepared for: Precision Dynamics Corporation

By: Michael L. Beigel Beigel Technology Corp.

Date: March 3, 2000 REVISED: April 17, 2000

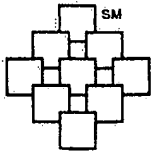
DRAFT ONLY: NOT FOR DISTRIBUTION

SUMMARY:

This report includes specifications and circuit diagrams for RFID tags that could be fabricated directly on flexible substrates using organic or other thin film semiconductor devices.

The schematic diagrams included in this report depict 4-bit read-only tag examples.

— Copy #1 of 6 PD Walter Koshen —



1. Specifications for Example RFID tags

READ-ONLY System Operation: The example tag system must be capable of receiving power from the RFID reader to the RFID tag via inductive coupling, and transmitting data from the tag to the reader also via inductive coupling.

Activation Field Frequency: The activation field frequency may be from under 100 KHz up to over 30 MHz.

Demonstration tags: For demonstration purposes we can tolerate a large antenna coil, short reading distance, minimum number of data bits, and non-standard operating frequency. The only requirement is demonstration of operation and data transmission.

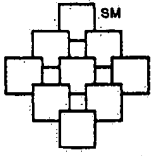
Commercial Tags: For commercial purposes we are targeting a wristband size antenna, reasonable reading distance, commercially viable number of data bits and operating frequency compatible with international unlicensed standards.

The complexity of the tag designs will increase with increased data storage capability, reliable reading range and other issues affecting the stability of commercial products.

Detailed specifications for the tags are beyond the scope of this report. Examples of commercial RFID tag and IC specifications from companies such as Philips provide a notion of the detail level required in the specification.

See Appendix 1 (TEMIC RFID Tag Specification)

READ-WRITE System operation: For a Read-Write system, additional signal processing and data storage architectures are needed in the tag. The tag must contain means to detect and demodulate data and control signals from the reader, and program received from the reader into a one-time-programmable or re-programmable nonvolatile data memory in the tag. A subsequent report will provide system and circuit details for demonstration read-write systems.



2. Circuit Elements for Example RFID Tags

Read-Only Tag Circuit Components:

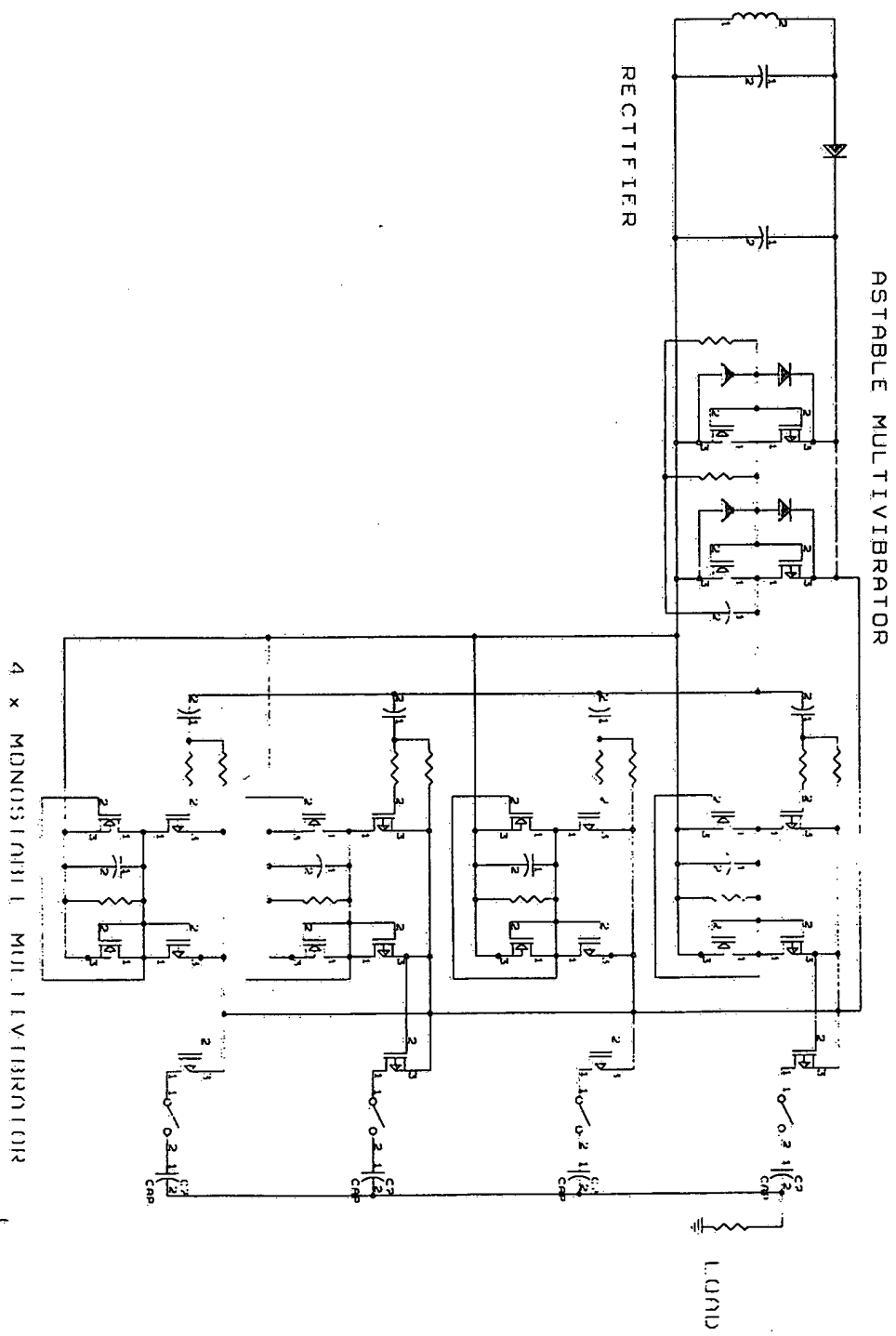
For operation of the RFID tag, the following circuit components must be fabricated on the substrate:

- Inductor Antenna Coil
- Resonance Capacitor
- Rectifier diode
- Charge storage capacitor
- P-type FET
- N-type FET
- Resistor to ground
- Resistor isolated from ground
- Capacitor to ground
- Capacitor isolated from ground
- Wire to ground
- Wire isolated from ground
- Insulating layer
- Inter-layer wire
- Data Element (pair of conductive pads optionally connected by conductive strip)

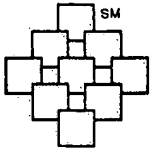
Read-Only Tag circuit elements:

The electronic components listed above must be combined to form circuit "blocks" which provide the RFID function:

- Resonant Inductor antenna
- DC Power extractor
- Loading element
- Complementary transistors
- Timer or counter
- Monostable Multivibrator
- Astable Multivibrator
- Schmitt Trigger
- Flip-flop
- Logic gates
- Data memory elements (read-only nonvolatile)



| | |
|-------------------------------|-----------------------|
| Title | |
| OR 1011-11 COMB ONLY COMP | |
| CLININT. CH | |
| Demonstration Tag - Version 1 | |
| Size | Document Number |
| B | |
| Date | Dec 11, 5, 2000 Sheet |
| REV | A |
| of | 1 |



Version 2: Four bits. Direct modulation, internal clock, counter

This circuit employs an internal astable multivibrator which functions as the master clock. The multivibrator time constant is derived from an internal R-C reference, and not from the external field frequency. The clock signal drives a series of flip-flop stages, forming a four bit repeating timer. The 16 decoder sections each provide one output logic "High" pulse for each sequential state of the timer. Each decoder output may be programmed by connecting its "switch" pads to the internal load with a conductive ink spot. The "high" pulse of each connected set of switch pads will provide a loading of the tag circuit power consumption. Thus the tag will output a sequence of loading pulses corresponding to the programmed tag code.

Antenna: L-C parallel

Rectifier: Single Diode

Clock: Free-running astable multivibrator

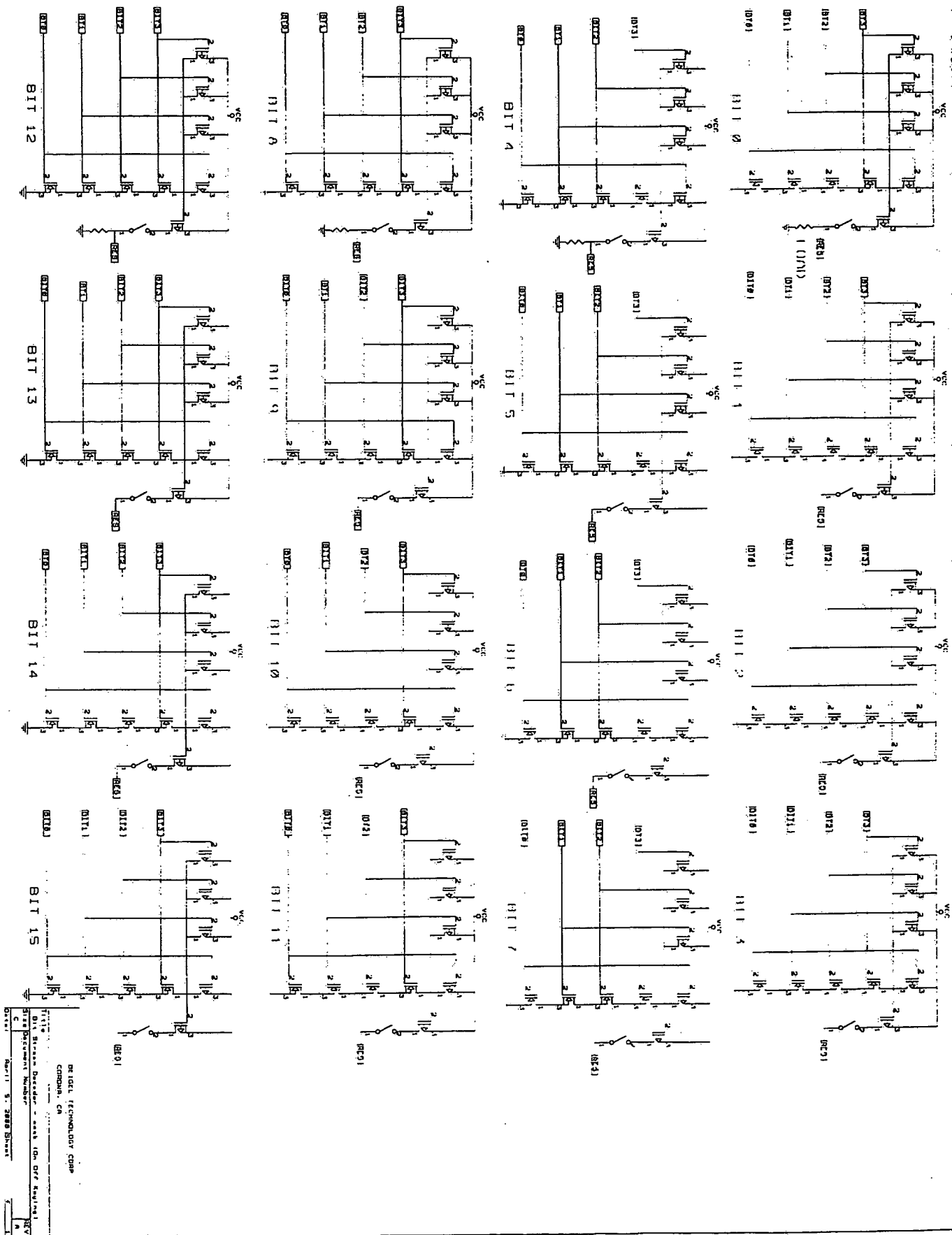
Sequence Generator: four stage binary counter,

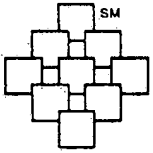
Data Address Decoder: 4 input-16 output de-multiplexer

Data programming: connecting or not connecting load to Data Address Decoder outputs

Modulator: internal load connected to data address decoder outputs

Circuit Diagram: Diagram 2 (Page 5A, Page 5B)





Version 3: Four Bits, Direct modulation, field-derived clock, counter

This version uses a fast Schmitt trigger clock generator to derive a clock pulse from (and thereby synchronous with) the power signal from the reader field. The clock generator is followed by three flip-flop pre-scaler stages to subdivide the field clock frequency and derive the data readout frequency. Then the divided clock passes through additional flip-flop dividers, which are coupled to a 4-bit input to 16-output demultiplexer. The data is programmed by connecting the decoder switch pads with conductive ink spots. The tag data modulation is similar to the tag of Version 2, except that the modulation is synchronous with the reader activation field frequency.

Antenna: L-C parallel

Rectifier: Single Diode

Clock: Free-running astable multivibrator

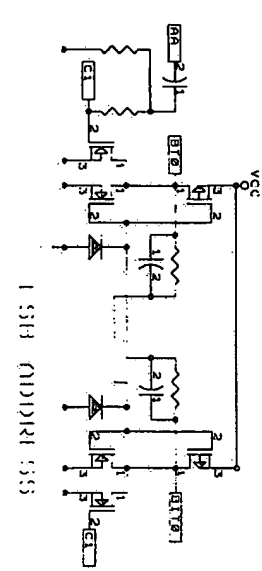
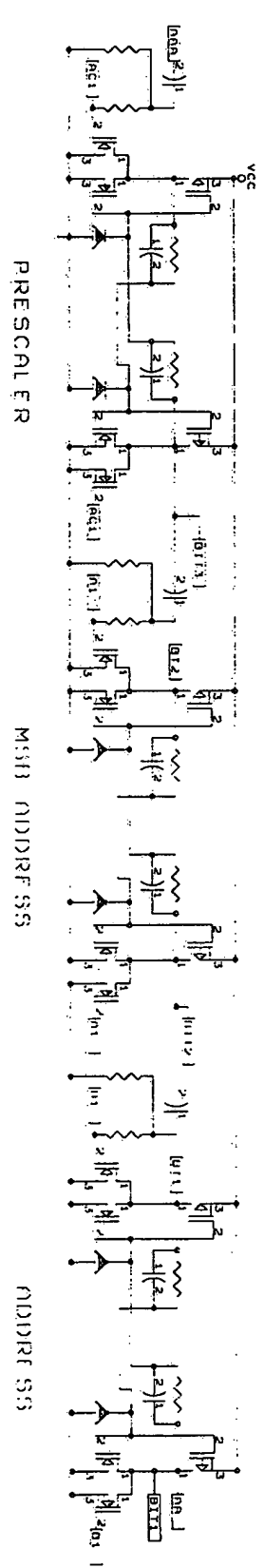
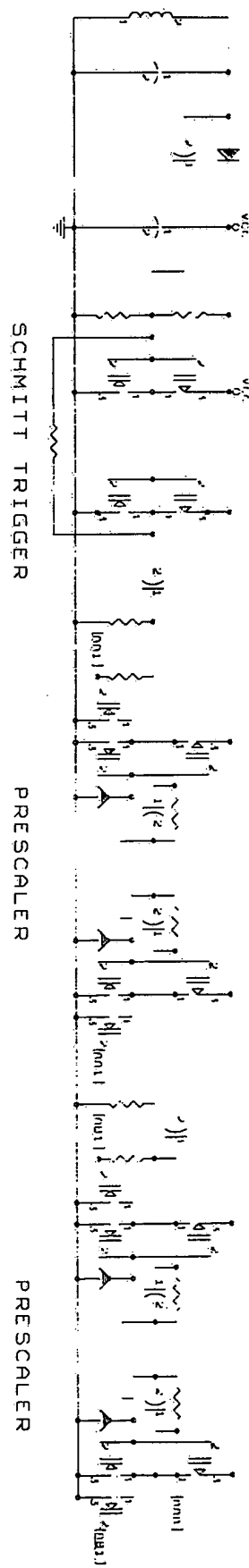
Sequence Generator: four stage binary counter, 4 input-16 output multiplexer

Data programming: connecting or not connecting load to multiplexer outputs

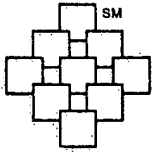
Modulator: internal load or FET connected across antenna coil terminals

Clock: divider from field coil (Schmitt trigger, N-stage counter feeding 4bit counter)

Circuit Diagram: Diagram 3 (Page 6A and 6B)



| | | | |
|-------------|--|----------|--|
| Title | | Revision | |
| Description | | Date | |
| Author | | Checked | |
| Drawn | | Approved | |
| Project | | Sheet | |
| Part | | Total | |
| Revision | | Date | |
| Description | | Revision | |
| Author | | Checked | |
| Drawn | | Approved | |
| Project | | Sheet | |
| Part | | Total | |
| Revision | | Date | |



Version 4: Four Bits, Redundant modulation

This version contains the circuitry of version 3, plus an additional modulator stage driven by data and clock, to produce a phase-shift keyed (PSK) modulated signal derived from the field frequency. Alternative synchronous modulator circuits could also provide Differential Bi-Phase, Frequency-Shift-Keyed or similar redundant modulation methods synchronous with the reader field frequency.

An alternative version could substitute the astable clock from Version 2 for the Schmitt trigger and prescaler stages. This would deliver a redundant modulation asynchronous and independent from reader field frequency.

The present version provides data modulation by combining the clock frequency divided by four (output of the second pre-scaler stage) in an EXOR gate with the logic output of the sixteen-output demultiplexer. Thus every time the data changes from 1 to 0 or from 0 to 1, there will be a phase change in the modulation.

Antenna: L-C parallel

Rectifier: Single Diode

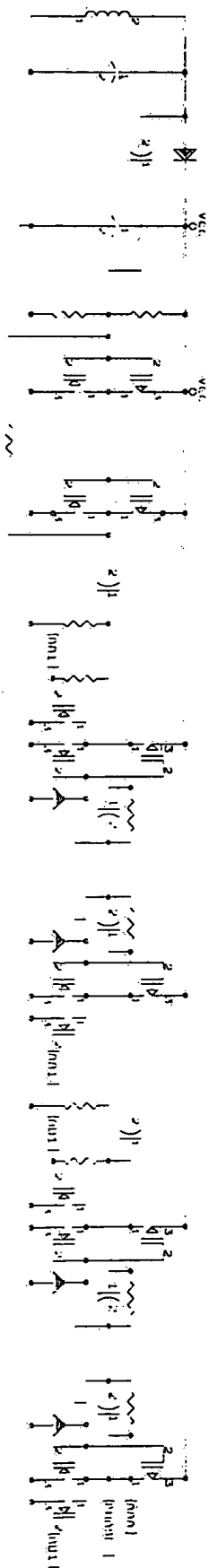
Clock: Free-running astable multivibrator

Sequence Generator: four stage binary counter, 4 input-16 output multiplexer

Data programming: connecting or not connecting load to multiplexer outputs

Modulator: EXOR PSK modulator (sub carrier = carrier/4, data = sub carrier /16)
internal load

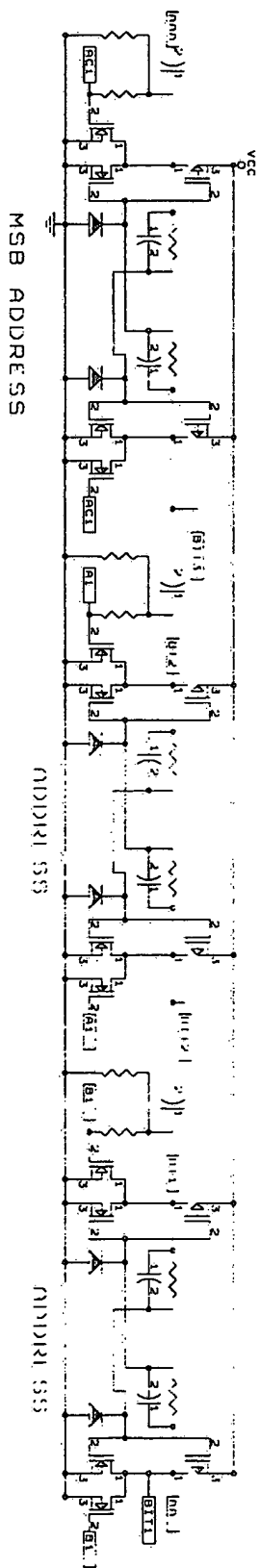
Circuit Diagram: Diagram 4 (Page 7A, 7B)



SCHMITT TRIGGER

PRI SCOLLER

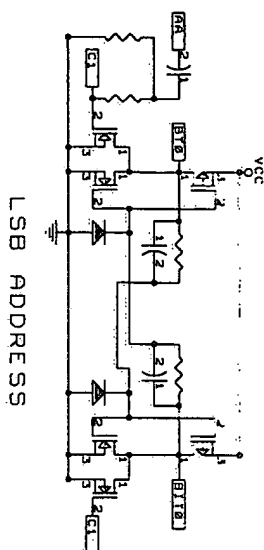
PRI SCOLLER



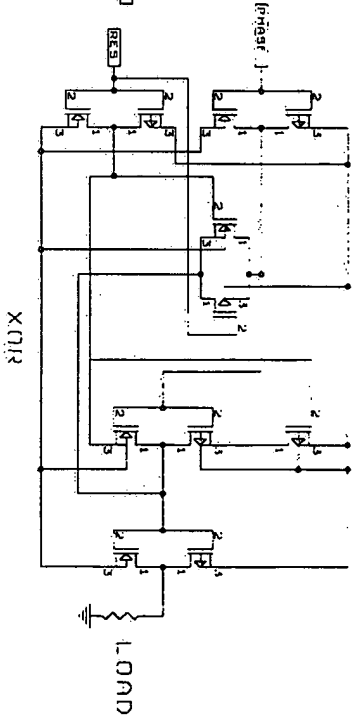
MSB ADDRESS

ADDRESS

ADDRESS



LSB ADDRESS



XOR

| | |
|-------------|-------------------------------|
| TITLE | DEMONSTRATION TAP - VERSION 4 |
| CORPORATION | CORONA, CA |
| REV | 1 |
| DATE | 10/1/77 |
| BY | J. H. HARRIS |
| CHECKED | J. H. HARRIS |
| APPROVED | J. H. HARRIS |

Memorandum

PRECISION DYNAMICS CORPORATION

Date: 03/20/00

To: Walter Mosher, Bob Kraemer, Ozzie Penuela, Nick Curtain, Paresh Davda,
Bob Shaub, & Barry Weinstein

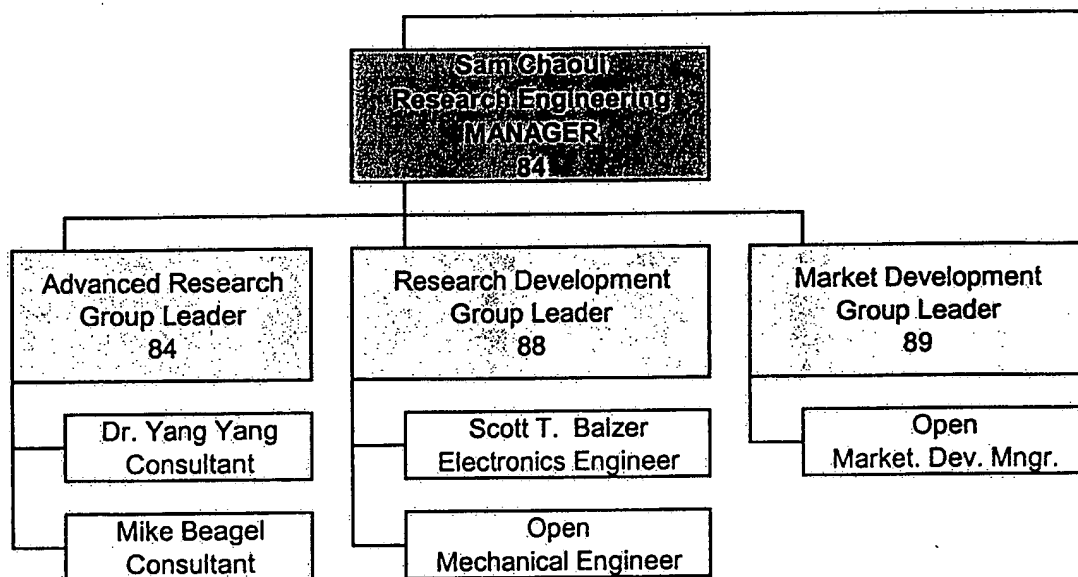
From: Sam Chaoui

Subject: **Engineering Organizational Chart Binder**

This binder gives you an overview of the restructure of the Engineering Department. It includes: Organization Chart, Department Functions descriptions, a Master Project List for the Year 2000, and one of the new forms in the Engineering Department.

We are presently in the final review phase of a new Engineering workflow system along with all associated forms and procedures. They will be released shortly, at which time, your binder will be updated.

Thank you.



ENGINEERING DEPARTMENT

Department Functions

ADVANCED RESEARCH - Department 84

The department is charged with the responsibility to continuously survey the universe of technology and investigates developments that can lead to innovative products. A primary function is establishing contacts and relationships with entities and individuals that are close to the focused areas of technical change. Additionally, a constant review of focus efforts is required to insure that the needs of the corporate strategic plan are being served. In order to develop information, the department will utilize a combination of individual consultants, research firms, government agencies and/or university or industry experts. The department is staffed by doctors, scientist and advanced engineers that have experience in multiple areas of technology.

Activities include:

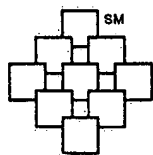
- Postulate the direction and importance of technology developments.
- Propose recommendations for further resear efforts on focused developing technology.
- Develop comprehensive analysis and make recommendations.

RESEARCH DEVELOPMENT - Department 88

This department takes the approved technology trend investigation and completes an analysis of the feasibility of utilizing the technology in a product or process. The analysis can be in the form of internal or external development, evaluating and testing the outlined technology. The output of this unit can be the recommendation to proceed with implementation or to take no action. The department oversees the analysis output of the department but the development of the analysis may be completed by outside consultants if necessary. Staffing includes engineers with advanced experience in multiple disciplines, designers, drafters and laboratory technicians.

Activities include:

- Design and development of prototype demonstration samples of products and equipment.
- Testing of samples to prove feasibility with laboratory and or beta test programs.
- Documenting program results and makes recommendations for possible implementation.



**BEIGEL
TECHNOLOGY
CORPORATION**

www.beitec.com

• PHONE: (760) 633-3868
• FAX: (760) 633-3819
• E-MAIL: beigel@beitec.com

308 VIA JULITA • ENCINITAS, CA 92024

PRECISION DYNAMICS CORPORATION

POLYMER RFID PROJECT

PROPOSED YEAR 2000 PROJECT ACTIVITIES UPDATE JUNE 2000

ALL PAGES CONFIDENTIAL MATERIAL

Prepared for: Precision Dynamics Corporation

By: Michael L. Beigel Beigel Technology Corp.

Date: June 2, 2000 REVISED: June 20, 2000

SUMMARY: Proposed strategy for development of an RFID tag on a flexible substrate, year 2000 activities.

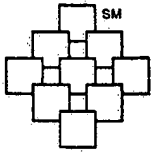
Updated June 2000 in light of recent project activities and IP search.

Original report (January 31, 2000) is in black text.

Update suggestions are in red text.

1. Technology and Intellectual Property activities
2. R&D activities
3. Level of Effort

✓
Distribution: W. Mosher, O. Penuela, T. Mahoney, S. Chaoui, M. Beigel



1. Technology and Intellectual Property Activities

1.1 Inventions and patents:

UPDATE: BTC recommends the following:

1. Brainstorm for patent applications again.

Pursue all presently pending patent applications. New areas of desired patent coverage should be defined. Continue efforts to generate and evaluate invention ideas and prepare new patent applications.

Scan the industry for potential infringers of issued patents, look for potential licensees for issued patents.

1.2 Knowledge of emerging Technology, products and intellectual property:

UPDATE: BTC recommends the following:

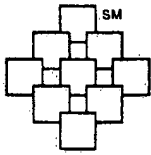
1. We should update patent and web search again for poly/flexible electronics

Perform quarterly update searches of scientific and technical journals, WWW publications, US and international patents. The searches may be based on known "key-words" and information resources developed in our previous research, but should be continuously expanded to cover new search terms and information resources.

Search products announced in relevant technology areas, and acquire and analyze products or samples that appear particularly relevant.

Search for new suppliers and new offerings by existing companies in relevant fields.

Product review procedure: Obtain and analyze new RFID products for relevant technology.



2. R&D Activities

UPDATE: BTC recommends the following:

1. Yang polymer memory project approved. BTC will support the project as needed with test fixtures, functional tests, and support electronics.

2. Breakthrough needed: printable diode which will have performance at 13.5 MHz and low voltage drop. This is probably the key development item. Once a diode is developed, work on a resonant antenna and power supply should proceed.

2.1 Polymer diode project: Continue with the polymer diode project with Prof. Yang. The next few steps would be:

Polymer diode on flexible substrate: Make and test the polymer diode on a flexible polymer substrate instead of the glass substrates we have been using.

Rectifier and storage capacitor combination: Make and test a combination polymer rectifier and charge storage capacitor on a single substrate. Start with glass substrate and transfer to flexible polymer substrate.

Resonant antenna, rectifier and storage capacitor (=Power Supply): Using a 125 KHz resonant frequency structure, make a wire-wound antenna coil and resonant circuit with polymer rectifier, charge storage capacitor and resistive load.

Change effort to direct toward 13.56 MHz system!

Power supply plus simple encoder and signal generator (=minimum RFID tag): A low-voltage silicon semi-custom chip with clock extractor, counter and decoder, load transistor, and external pads to connect with printable-programmable encoder.

2.2 Demonstration RFID TAG ON FLEXIBLE SUBSTRATE with no silicon:

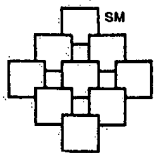
NOTE: THIS IS A LONG RANGE OBJECTIVE. It is for a demonstration prototype rather than a production item.

Design and produce all the circuit elements required for a printed RFID tag.

Combine the elements to produce minimum RFID tag prototype.

Develop methods of mass production for tags.

Design RFID reader.



Tag circuit elements:

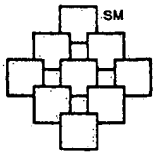
- Inductor antenna
- Resonance capacitor
- DC Power extractor
- Loading element
- Complementary transistors
- Timer or counter
- Logic gates
- Data memory elements
- Interconnect wires, vias, bridges

2.3 Fabrication Methods

Investigate present methods of fabricating polymer electronic and other potentially "printable" electronic technologies for flexible substrates. Devote efforts specifically towards developing production fixtures and methods for economical mass production.

UPDATE: BTC recommends the following:

We should perform a thorough search on polymer and other printable semiconductor manufacturing methods, patents, material suppliers, production companies.



3. Level of Effort

Proceed with R&D using PD internal funding and possible "Grant" funding.

3.1 Activities

Pursue pending patent applications, including the new material generated during the last project phase (April-December 1999). New Yang polymer memory ideas.

Perform technology and IP update studies quarterly. Keep doing this!

Continue "brainstorming" efforts to generate new patent applications based on emerging technology possibilities and inventive thoughts. Another intensive effort needed.

Pursue the Yang "polymer diode" project per his proposal of January 18, 2000. Focus on an idea and method for a diode that works at 13.5 MHz.

Develop the "minimum" RFID tag on flexible substrate using no silicon components. Detailed project plan and budget would be developed, including provision for laboratory facilities, materials and expertise needed. Suspend until we have the 13.5 MHz diode.

3.2 Funding

PD may use internal funding only to prevent any dilution of equity or intellectual property rights. Additional funding such as US government grants can be obtained in connection with universities such as UCLA and top researchers such as Prof. Yang. With additional funding and "no-cost" lab facilities, PDC could pursue a greater effort.

PD should recommend a level of funding, and we will work within it.

3.3 BTC availability:

Mike Beigel: 8-20 hours per week as needed

Other BTC: as needed

Memorandum

PRECISION DYNAMICS CORPORATION

Date: 06/05/00

To: Dr. W. Mosher, T. Mahoney, M. Beagel, O. Penuela, B. Berman,
D. Peterson, S. Balzer, T. Schmidt

From: Sam Chaoui 

cc: Bob Kraemer

Subject: **RFID Status Meeting Action Items – FOLLOW UP**

This memo addresses the action list as discussed in the RFID team meeting of June 2, 2000 and as a follow up to the May 31st meeting with the above attendees.

1. Send a sample package of all discussed RFID Bands to Mr. Mahoney. They will be numbered and a description attached for reference

Scott B. - Monday 6/5/00

Send the package out to Dr. Mosher first for approval and then forward it to Mr. Mahoney.

2. Determine assignees for patent application and submit to Mr. Mahoney.

Scott B. - Monday 6/26/00

The following were identified as possible innovative (patentable) ideas or concepts with the corresponding inventors. Scott will coordinate the writing of the disclosures.

- a) Method of inlet installation via lamination and encapsulation - S. Balzer, G. Soltes
- b) Inserting inlet into Superband and heat sealing end as encapsulation method - O. Penuela and J. Castelblanco
- c) Conductive band for tampering detection - A. Bekker for assembly method but original idea came from E-Code systems.
- d) Co-extruded fiber optic within the band material for conductivity - S. Balzer
- e) RFID inlet integrated within an adhesive (std. or UV curable), heat laminating label - S. Chaoui, O. Penuela
- f) Laminating inlet within a Compuband/Superband similar to a) above - J. Castleblanco and I. Toth
- g) Printing conductive ink antennas on band along with a polymeric chip - TBD

3. Establish and publish a price point for each product along with Gross Profit Margin (GPM)

Tim S. – June 17, 2000

Memorandum

PRECISION DYNAMICS CORPORATION

Date: 02/14/01

To: Dr. Mosher

From: Sam Chaoui

Cc: Ozzie Penuela

Subject: **RFID Meetings**

In confirmation of our conversation regarding the RFID Bi-monthly meetings, following are the dates and times as agreed. Of course, we will always meet right after the monthly Engineering staff meeting with you. (Last Thursday of the month, included in the table below.)

Per your instructions, we will decide on following meetings when we get closer to mid-April.

| February | March | April |
|-------------------|-------------------|-------------------|
| 2/22 @ 10:30 a.m. | 3/2 @ 12:30 p.m. | 4/13 @ 10:00 a.m. |
| | 3/29 @ 10:30 a.m. | 4/26 @ 10:30 a.m. |

Thank you.

SC/hl

Memorandum

PRECISION DYNAMICS CORPORATION

Date: 04/18/01

To: Distribution

From: Sam Chaoui

Cc: Walter Mosher, Robert Kraemer

Nick Curtin, Paresh Davda, Ozzie Penuela, Bob Shaub, Barry Weinstein

Subject: **RFID Project Management**

Apart from any production issues, regulatory audits, any safety or other critical projects, RFID remains PDC's number one development project.

Due to the ever-increasing workload that the existing project management is facing, Ozzie and I have come up with the decision to recruit an RFID project manager. Because of the specific and required high-technical and managerial requirements of this position, it may take a few weeks to locate a suitable candidate. Meanwhile, the project is still moving at a fast pace and requires daily maintenance.

After considerable evaluation, I was authorized and am pleased to announce that Ron Fullerton will be taking over the responsibility of this position on an interim basis until a permanent candidate is recruited. Ron will divide his time between RFID and his current duties as group product manager for hospital wristbands. Nick is also in full support of this move.

Ron will be responsible for all aspects of the RFID project management including all personnel task assignments. He will develop the project Gantt schedule and chair the weekly meetings. Please coordinate your activities directly with him. Ron will report to me on this project, but I will continue to oversee all financial approvals.

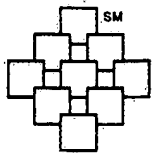
Please welcome and give Ron your full support.

If you have any questions, please see me.

Thank you,

SC/hl





RFID PROJECT

PRECISION DYNAMICS CORPORATION

ISO/IEC STANDARDS PERTAINING TO RFID PROJECT

ALL PAGES CONFIDENTIAL MATERIAL

| | | |
|---|--------------------------|--------------------------------|
| Prepared for: Precision Dynamics Corporation | | |
| By: | Michael L. Beigel | Beigel Technology Corp. |
| Date: | May 2, 2001 | |

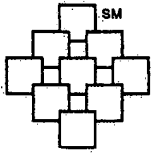
SUMMARY:

First report on standards applicable to Precision Dynamics RFID product line.

Some ISO/IEC standards obtained and summarized.

Suggestions for further activities.

DISTRIBUTION: PD INTERNAL, Ozzie Penuela to distribute



INTRODUCTION

RFID product marketability and interoperability is substantially determined by voluntary and mandatory standards and regulations.

The development RFID field (technology and markets) has been historically limited by ambiguity of the standards, the credibility of companies claiming compliance with the standards, and the technical/corporate/political factors involved with setting and monitoring the standards.

Some regulatory standards, such as are imposed by FCC and international regulatory authorities, determine legal limitations on the use of RFID technology outside certain frequency ranges and power limits.

Other standards attempt to enhance the marketplace by defining standards of interoperability to be satisfied by multiple sources of product supply, but do not constitute legal limitations.

Since the core technologies are in a state of flux and the supply of product is presently limited by the ambiguous state of the standards, the knowledge of and prediction of the standards is critical to all aspects of RFID product development.

OBJECTIVES OF STANDARDS STUDY

The primary objectives of this study are to determine which national and international regulatory and voluntary standards are relevant to PD's RFID product line development efforts, and to begin an ongoing effort at implementing these:

1. Anticipate preferred technologies and suppliers based on standards.
2. Understand the standards organizations applicable to PD's RFID efforts
3. Acquire potentially relevant standards documents
4. Preliminary analysis of standards documents
5. Purchase compliant components and sub-assemblies for use in products.
6. Legal ability to sell finished (compliant) PD products
7. Strategy for participation in standards groups relevant to PD business interests

The objectives should be reviewed and amended as appropriate.

3.1.2 Byte

A byte consists of 8 bits of data designated b1 to b8, from the most significant bit (MSB, b8) to the least significant bit (LSB, b1).

3.2 Abbreviations

| | |
|-------|----------------------------------|
| AFI | Application family identifier |
| CRC | Cyclic redundancy check |
| DSFID | Data storage format identifier |
| EOF | End of frame |
| LSB | Least significant bit |
| MSB | Most significant bit |
| RFU | Reserved for future use |
| SOF | Start of frame |
| UID | Unique identifier |
| VCD | Vicinity coupling device |
| VICC | Vicinity integrated circuit card |

READER
TAG

3.3 Symbols

→ f_c Frequency of operating field (carrier frequency)

4 Definition of data elements

4.1 Unique identifier (UID)

The VICCs are uniquely identified by a 64 bits unique identifier (UID). This is used for addressing each VICC uniquely and individually, during the anticollision loop and for one-to-one exchange between a VCD and a VICC.

The UID shall be set permanently by the IC manufacturer in accordance with figure 1.

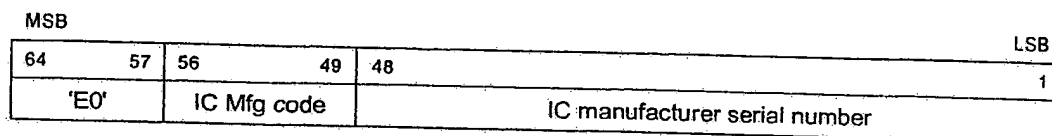


Figure 1 — UID format

The UID comprises

- The 8 MSB bits shall be 'E0',

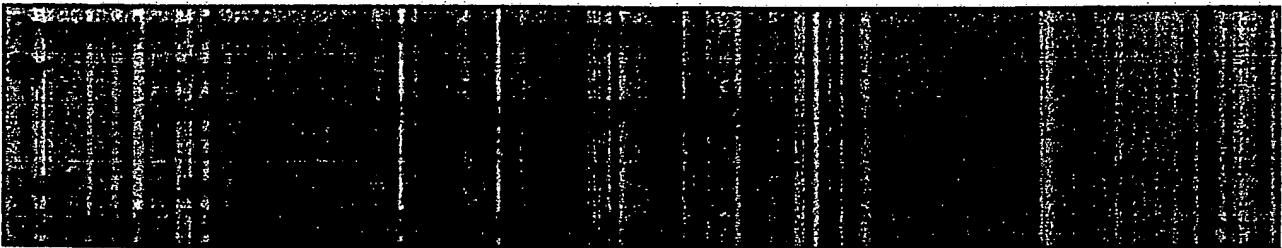
CONFIDENTIAL

PRECISION DYNAMICS CORPORATION
POLYMER RFID PROJECT

Wristband Patch Antenna

ALL PAGES CONFIDENTIAL MATERIAL

*Reviewed
MB
7-2-01
see comments*



DRAFT ONLY: NOT FOR DISTRIBUTION

FIELD OF THE INVENTION

This invention relates to radio-frequency identification (RFID) tags used in identification wristbands, and in particular to the use of a microstrip patch antenna to improve the operating range between tags and tag readers.

*Need to review MB
6/13 drawings and
check for inclusion in
disclosure text*

BACKGROUND OF THE INVENTION

Low power radio-frequency identification (RFID) systems can operate over a wide range of frequencies, including the high-frequency (HF) through super-high-frequency (SHF) radio bands, roughly 3 MHz through 6 GHz. Information is stored electronically in a transponder or RFID "tag" and that information is communicated to a tag "reader." Communication between the RFID tag and reader is by the transmission and reception of electromagnetic (EM) waves, and each must have an antenna to convert electrical signals to EM waves and vice versa. One important use for identification wristbands is patient identification and location in hospitals, clinics, and other locations; in conjunction with an appropriate reader, patient information can be collected electronically and used by the medical staff in performance of their duties. Other uses include veterinary medicine, temporary security measures, and facility access control.

Identification wristbands typically consist of a flexible wrist strap having a length greater than its width, and a closure or securement device for attaching and maintaining the wristband securely around the wearer's wrist. A portion of the wristband is used for imprinting or otherwise attaching identification or other information regarding the wearer. Various wristband

constructions, attachments and other features are described in (include precision dynamics patent numbers).

PRIOR ART PATENTS FOR TUTTLE PATCH DISCLOSURE

MB June 13, 2001

US patent 6,215,402 (Rao et al) describes a RFID transponder employing a patch antenna and an impedance matching circuit.

US patent 6,181,287 (Beigel) describes reactively coupled circuit elements formed on a flexible substrate for use in RFID wristbands.

US patent 6,127,977 (Cohen) describes a microstrip patch antenna with fractal structure.

US 6,111,549 (Feller) describes a flexible circuit antenna and method for manufacturing.

US patent 5,995,048 (Smithgall) describes a quarter wave patch antenna for an RFID system.

US 5,973,600 (Mosher) describes an RFID device formed of a plurality of laminae which bear the components of an RFID circuit.

US 5,973,598 (Beigel) describes a RFID tag, including antenna and operative circuitry formed directly on a flexible substrate.

US 5,799,426 (Peterson) describes a uniform thickness adhesive closure for an identification bracelet.

US 5,740,623 (Juhan et al) describes a tubular identification wristband with a separate connector as securement element.

US 5,609,716 (Mosher) describes apparatus for manufacturing and dispensing identification wristbands.

US 5,581,924 (Peterson) describes a pocket style identification bracelet that can store an identification device.

US 5,493,805 (Penuela) describes a memory chip holder for an identification wristband.

US 5,479,797 (Peterson) Describes a unidirectionally sizeable bracelet assembly and closure means.

The performance of an RFID tag operating in the HF band, for example at 13.5 MHz, is generally not affected by proximity to the human body. This is a desirable property for RFID tags

CONFIDENTIAL

used in identification wristbands. Coupling between the tag and reader antennas is primarily by the magnetic component of the reactive near field, in which the tag antenna is configured as a coil in a resonant circuit. However, a typical wristband is six inches in length which must include an antenna, while the wavelength at 13.5 MHz is 73 feet, and it is well known that antennas which are a small fraction of a wavelength in linear dimensions are very inefficient radiators and receptors. As a result, the useful range of operation is very limited, sometimes just a few inches from the reader antenna. This is a significant disadvantage which may limit the usefulness of the tags in identification wristbands, and may render them unuseable, for example, in personnel location or ingress/egress alarm applications.

RFID systems may also operate at much higher frequencies, including operation at or in the vicinity of 400 MHz, 915 MHz, 2.45 GHz in the ultra-high frequency (UHF) band and 5.88 GHz in the SHF band. At these frequencies, coupling between tag and reader antennas is by the radiating far field, which is the EM wave that propagates over distances of more than a few wavelengths. These frequencies correspond to wavelengths from 30 inches down to 2 inches, which are much more suitable, in terms of efficiency, for antennas in a wristband or other structure of comparable size. As a result of the more efficient antennas, operation at these frequencies may result in substantially higher ranges, typically up to ten feet or more. However, compared to the HF band, radiation and reception of EM waves at these higher frequencies bands are affected much more strongly by obstacles and materials in the immediate environment of the antenna as a result of the shorter wavelengths. In particular, a loop or dipole antenna, operating on or adjacent to the human body, for example in a wristband, will be severely detuned and possibly rendered inoperable, with a commensurate degradation of the communication link. Thus the useability of these antennas in identification wristbands with RFID capability is very limited.

The aforementioned antenna detuning and communication degradation are directly attributable to the fact that an isolated (free of nearby obstacles) loop or dipole antenna normally radiates EM energy in opposite directions. But, when on or near the surface of a human body, the reactive near fields (the electric and magnetic fields closest to the antenna) are distorted by the human tissue, causing an impedance mismatch between the antenna and the circuit to which it is immediately connected. This mismatch effectively detunes the antenna and reduces the amount of EM energy radiated in the direction away from the human body. It is therefore desirable to implement RFID capability in an identification wristband with an antenna having inherently reduced near-field energy on one side, toward the body, therefore radiating efficiently away from the body. It is also desirable that such an antenna be relatively thin so that it may be easily attached to or imbedded in an identification wristband and not be awkward for the wearer.

The type of antenna which meets these requirements is the microstrip or "patch" antenna. This antenna comprises a metallic patch, a dielectric substrate, and a ground plane, assembled into a flat antenna. This type of antenna can be manufactured in many ways, but it is typically fabricated from printed circuit board material having copper cladding on both sides. The antenna may be made small by using a thin substrate with a high dielectric constant. Maximum radiation from the patch antenna is normal to, and on the same side as, the patch, and minimal or no

Inductive =
?.

What about
FLEXIBLE
NAB 7/21

CONFIDENTIAL

radiation occurs on the opposite (ground plane) side. Undesirable proximity effects in a wristband RFID tag are therefore mitigated by placing the ground plane on the inner side toward the wearer. The antenna may be separately attached to a wristband or integrated into the electronic circuits in a wristband. The antenna may also be constructed with a flexible printed circuit board so that it will bend as part of the wristband. (WHAT IS IN THIS PARAGRAPH IS REPEATED EITHER IN THE SUMMARY OR IN THE DETAILED DESCRIPTION. IT IS USED HERE FOR BACKGROUND INFORMATION.)

SUMMARY

The invention disclosed herein is an identification device in the form of a wristband or bracelet, adhesive patch, or other wearable appliance, operating in the UHF ^{through} or SHF radio bands, which includes electronic RFID circuitry employing an attached or embedded microstrip or patch antenna. The RFID circuitry may be mounted between the patch and ground plane, either in the dielectric or attached to either conductor's interior surface. The RFID circuitry may also be mounted on the underside of the ground plane, on the top side of the dielectric and adjacent to the patch, or on the top side of the patch. The patch antenna may be curved instead of planar or constructed using a flexible substrate material, and it may be imbedded between layers of the wristband or other appliance.

Part of the antenna structure may be contained in or be integral to the securement means for the wristband. For example, any or all of the ground plane, the antenna radiating surface, the RFID circuitry, the electrical connection between the RFID and both portions of the antenna may be integral to the securement means. The securement means may be fabricated either integral to or removable from the wristband strip (STRAP?) or other appliance.

BRIEF DESCRIPTION OF THE DRAWINGS (TUTTLE)

Figure 1. **Bracelet with microstrip antenna.** Figure 1 shows a bracelet containing a microstrip or patch antenna as a part thereof. It includes a top conducting plate, bottom conducting plate and a dielectric material in between. The antenna components are shown as connected or embedded as part of a bracelet strap.

MORE DETAIL NEEDED IN DESCRIPTION.

Figure 2. **RFID circuitry mounted within the dielectric material of the microstrip antenna.** Figure 2 shows the Radio frequency identification (RFID) components mounted in the dielectric on the bottom of the top plate, on top of the ground plane, or in between. Using bare die components allows the use of circuit elements as thin as 10 to 20 mils in height.

How's it connected to antenna?

Figure 3. **RFID circuitry mounted on the underside of the microstrip antenna.** Figure 3 shows the Radio frequency identification (RFID) components mounted on the underside of the ground plane. Using bare die components allows the use of circuit elements as thin as 10 to 20 mils in height.

Figure 4. RFID circuitry mounted next to the top plate. Figure 4 shows the RFID circuitry mounted on top of the dielectric, next to the top plate. A hole through the dielectric allows the RFID circuit to contact the ground plane under the dielectric.

Figure 5. RFID circuitry mounted on top of the top plate. Figure 5 shows the RFID circuitry mounted on top of the patch. A clearance hole through the top plate and the dielectric allows the RFID circuit to contact the ground plane under the dielectric.

Figure 6. A curved microstrip antenna. Figure 6 shows a curved microstrip antenna, allowing a better fit to the wearer. A bracelet may be attached to the antenna and circuitry as shown in figure 1.

Figure 7. Method of attaching the bracelet to the antenna and RFID circuitry. Figure 7 shows the antenna and circuitry laminated in between top and bottom non-conducting layers of bracelet material. The embedded antenna and circuit module are made beforehand or at the time of fabrication of the wristband product.

DETAILED DESCRIPTION

An identification wristband or bracelet in accordance with this invention is shown in FIG. 1. The microstrip or patch antenna includes the patch or top plate, a dielectric slab or substrate, and a bottom plate or ground plane. Mounted within the wristband and electrically connected to the antenna is a surface mount RFID chip containing electronic circuits. An RFID circuit consisting entirely of conductive, insulating and semiconductive materials directly deposited on the substrate may also be used.

The patch antenna is typically formed on a printed circuit board comprising a planar dielectric substrate of relative dielectric constant ϵ_r having copper cladding on one entire side of the substrate which forms a ground plane, and copper cladding on the other side which is etched to form a rectangular patch. The thickness of the substrate is typically on the order of one-hundredth of the free space wavelength of the radiated signal, and the patch itself is of length L and width $W < L$. When L is approximately a half wavelength in the dielectric substrate, the patch forms a transmission line resonator with open circuits at opposite ends. The ends of the patch resonator act as a pair of slot radiators because of the electric fields at the two open circuits. The far field radiation produced by this antenna will be strongest in the direction normal to the patch, with the electric field polarization in the plane of the patch and parallel to the length of the patch, i.e. a linearly-polarized (LP) EM wave. Both near and far fields will be minimum in the direction normal to the ground plane.

The antenna may be driven in many ways; two common methods are by a coaxial probe which protrudes through the ground plane and connects to the patch at a point centered halfway

CONFIDENTIAL

across the width W, and by a narrower microstrip transmission line which connects to the center of one end of the patch. *(KEEP THESE IN MIND FOR LATER DISCUSSION.)* The efficiency of a patch antenna, (ratio of radiated power to driving power) is very high (80 percent or more) for high quality substrates with low dielectric losses in the UHF and SHF bands. The common low-cost printed circuit board material, designated as FR-4, performs very poorly in these bands, although it may still be useable. High quality substrates for these frequencies are available from Rogers Corp., Chandler AZ.

CLARK CAN YOU SUGGEST A BETTER SUBSTRATE MATERIAL, EITHER RIGID OR PREFERABLY FLEXIBLE? MB

RIGID IS COVERED IN LAST SENTENCE ABOVE. I COULDN'T QUICKLY LOCATE UHF/SHF SUBSTRATES WHICH ARE FLEXIBLE ALSO. THE '402 PATENT MENTIONS FLEXIBLE SUBSTRATE BUT NOT IDENTIFIED. (THEY DID IDENTIFY FR-4)

When L and W are both approximately a half wavelength in the dielectric substrate, the antenna may resonate and radiate in two directions. Dividing the power equally between the two resonances but introducing a 90 degree phase shift between them, the resulting far field radiation, normal to the patch, will have an electric field which rotates in a circular pattern in the plane of the patch, i.e. a circularly-polarized (CP) EM wave. If the rotation of the electric field is clockwise in the direction away from the antenna, it is as a right-hand circularly-polarized (RHCP) wave, and if the rotation is counterclockwise, it is a left-hand circularly-polarized wave. The sense (RHCP or LHCP) is determined by the which direction in the patch leads by 90 degrees. The advantage of using CP radiation from a tag is that there is less dependence on antenna orientation when the reader antenna is either linearly polarized or circularly polarized with the same sense as the tag antenna.

It is preferred that the RFID circuitry be contained on a bare surface mount die which is 0.010 to 0.020 inch thick. The mounting of the RFID chip can be accomplished in several ways. It is necessary that the RFID chip is electrically connected to both the top and bottom plates (the patch and ground plane, respectively). When mounted on or adjacent to a plate, a direct connection (e.g. solder or conductive adhesive) is preferred between that plate and the chip. Methods of connecting to a non-adjacent plate include using wire, cable, or a printed circuit transmission line. The RFID circuitry may also be implemented directly onto the substrate, comprising printed circuits etched out of the cladding and discrete parts bonded to the circuits, connected to the antenna top and bottom plates using wire, cable, or a printed circuit transmission line.

MB ADD METHODS AND STRUCTURES FOR PROVIDING PART OR ALL OF PATCH ANTENNA IN SECUREMENT APPARATUS.

SEE COMMENTS BELOW RE. CLOSURE MECHANISM; IS THAT WHAT YOU MEAN BY "SECUREMENT APPARATUS?"

WHAT ABOUT FIGURE 1?

CONFIDENTIAL

SEE FIRST PARAGRAPH UNDER "DETAILED DESCRIPTION"

In FIG 2, the RFID chip is located in the region between the top plate and the bottom plate, including on the bottom surface of the top plate, the top surface of the bottom plate, and in the dielectric between the two. A wire may be used to connect through a hole in the dielectric to a plate. In this embodiment the chip is inside the resonating region of the antenna.

In FIG. 3, the RFID chip is shown mounted on the underside of, and directly connected to, the bottom plate. Connection to the top plate is by a wire passing through a hole in the dielectric. In this embodiment the chip is outside the resonating region of the antenna.

In FIG. 4, the RFID circuitry is shown mounted on top of the dielectric, next to the top plate. A hole through the dielectric allows the RFID circuit to contact the ground plane under the dielectric.

I HAVE SOME QUESTIONS RE. THIS EMBODIMENT. IF THE CHIP IS PLACED NEXT TO A RADIATING (END) EDGE, THEN THE HIGH ELECTRIC FIELDS AT THAT EDGE WILL BE DISTORTED BY THE CHIP, AND MAY ALSO INDUCE EMI ON THE CHIP CIRCUITS. IF THE CHIP IS PLACED NEXT TO A NON-RADIATING (SIDE) EDGE, THE DRIVING (NON-GROUNDED) LEAD SHOULD SOMEHOW GET CONNECTED TO THE CENTER OF A RADIATING EDGE OR TO A DRIVING POINT ON THE UNDERSIDE, AND DO SO WITHOUT SERIOUSLY DISTORTING THE FIELDS. I'M NOT SURE HOW TO MAKE AN ENABLING DISCLOSURE OF THIS.

FIG. 5 shows the RFID circuitry mounted on top of the patch. A clearance hole through the top plate and the dielectric allows the RFID circuit to contact the ground plane under the dielectric.

BUT HOW DOES THE DRIVING LEAD CONTACT EITHER A RADIATING END OF THE PATCH OR THE UNDERSIDE OF THE PATCH? SAME CONCERN RE. ENABLEMENT.

FIG. 6 shows a curved microstrip antenna, allowing a better fit to the wearer. The substrate may be flexible, or rigid and shaped with a curvature. A wristband or bracelet may be attached to the antenna and circuitry as shown in FIG. 1.

In the aforementioned embodiments additional non-conducting layers of material having low EM loss must be used to protect the antenna and RFID circuitry from moisture, abrasion, etc. An effective method to provide this protection is shown in FIG. 7, wherein the antenna and circuitry in the form of a substrate module are laminated in between top and bottom non-conducting layers of bracelet material. The embedded antenna and circuit module are made beforehand or at the time of fabrication of the wristband product.

THE ANTENNA OR A PART OF THE ANTENNA MAY BE FABRICATED AS PART OF THE CLOSURE MECHANISM (SECUREMENT MEANS) FOR THE WRISTBAND, OR WITHIN

THE CLOSURE MECHANISM OF THE WRISTBAND. THIS MAY BE COUPLED TO THE FLEXIBLE WRISTBAND BY ELECTRICAL OR REACTIVE COUPLING. MB
REMEMBER, THE ANTENNA SHOULD BE RADIATING AWAY FROM THE BODY. IF THE CLOSURE MECHANISM IS PLACED TOWARD THE BODY, AS WOULD BE EXPECTED (THAT'S USUALLY THE WAY IT IS WITH PRINTED NAME WRISTBANDS, ANYWAY) THEN THAT'S THE WRONG PLACE TO PUT THE ANTENNA.

IDEAS FOR CLAIMS

What is claimed is:

An antenna comprising:

1. a microstrip element made from flexible circuit materials; wherein said antenna is affixed to the patient; and is used for communicating patient identification
2. #1 -- communicating patient medical data
3. #1, 2 affixed as a bracelet
4. #1,2 affixed as an adhesive patch
5. #1, #2 ...has circuitry attached
6. #5 with battery
7. #5 without battery
8. #5,6,7 wherein circuitry is contained in the dielectric plane
9. #5,6,7 wherein the circuitry is affixed under the ground plane
10. #5,6,7 wherein the circuitry is affixed on top of the dielectric
11. #5,6,7 wherein the circuitry is affixed on top of the outer conductor of the microstrip element
12. veterinary
13. clinic
14. hospital
15. home
16. disposable,
17. non-disposable
18. rigid
19. curved
20. frequencies in the vicinity of 400 MHz, 915 MHz, 2.45GHz and 5.88GHz.
21. #1-16 where there are a plurality of elements.
22. #1-17 where the element is a continuous radiator.

CONFIDENTIAL

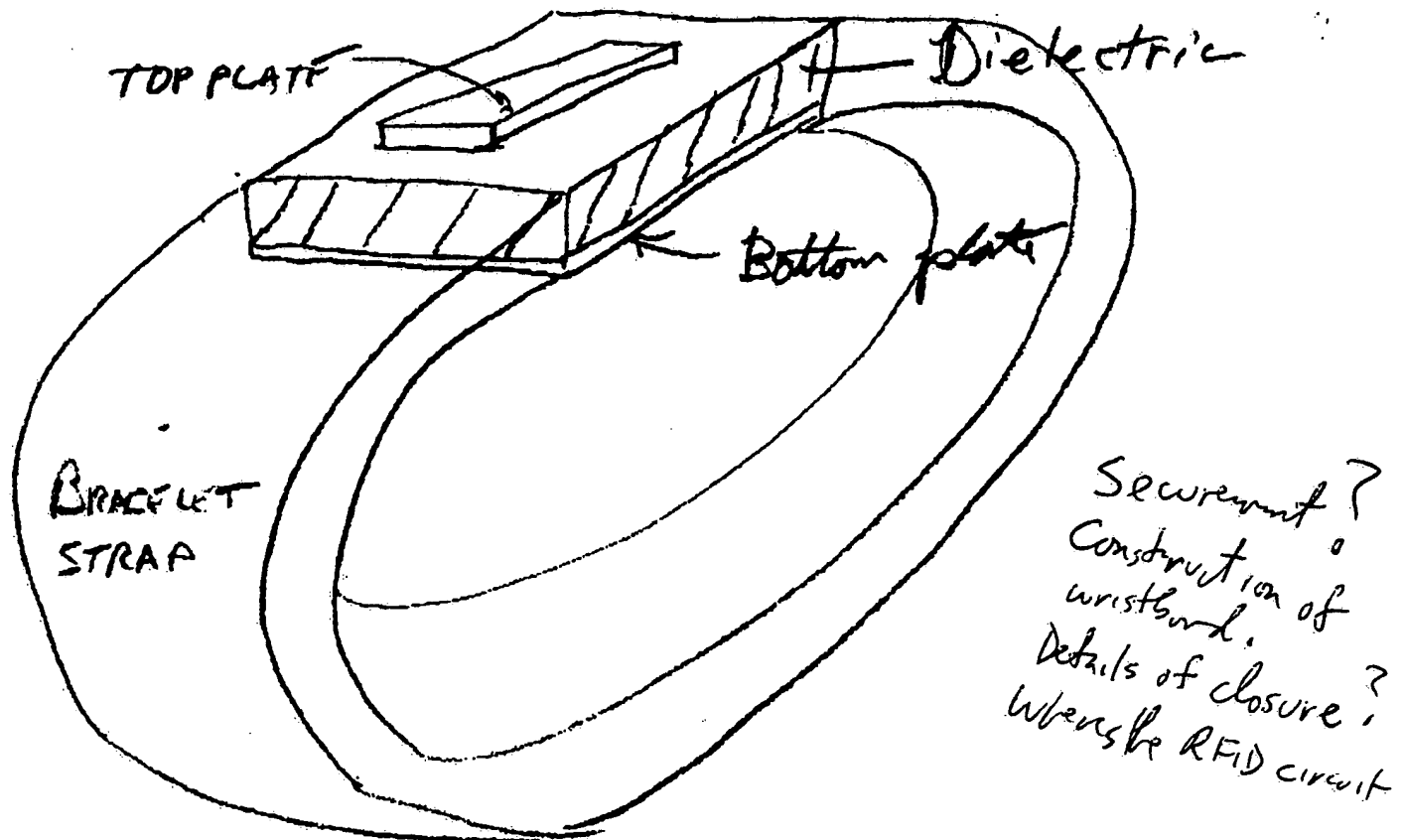
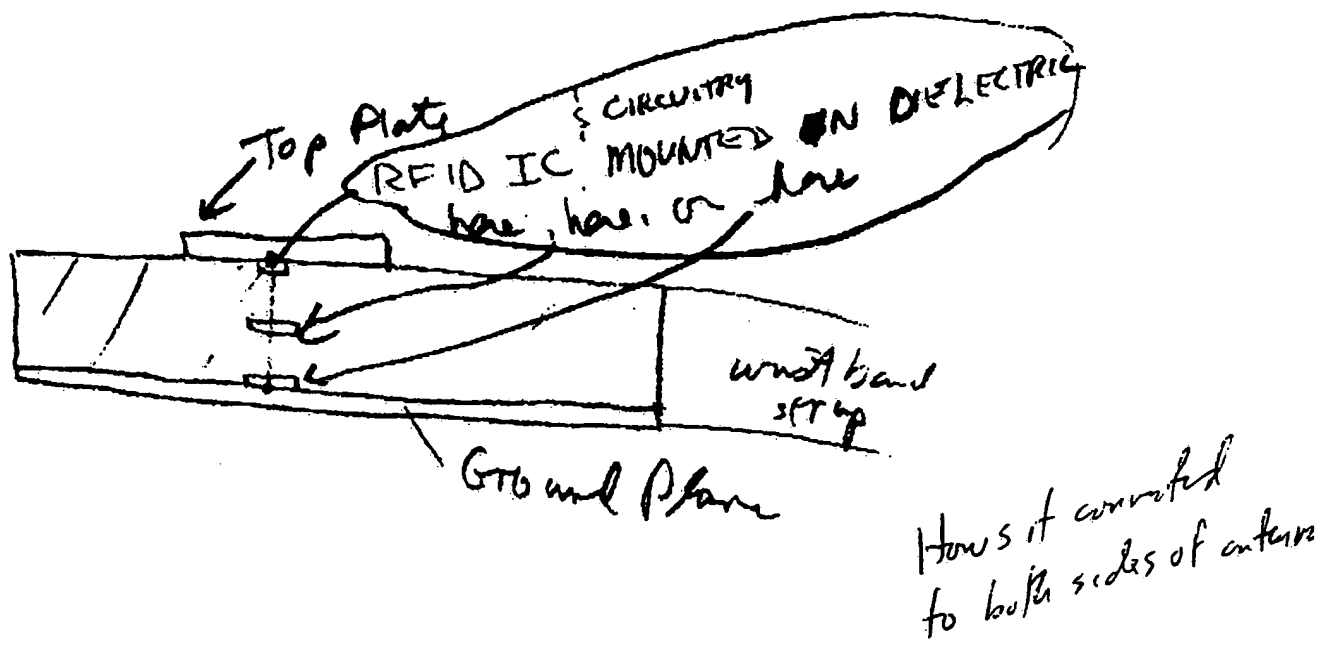


Figure 1. Bracelet with microstrip antenna. Figure 1 shows a bracelet containing a microstrip or patch antenna as a part thereof. It includes a top conducting plate, bottom conducting plate and a dielectric material in between. The antenna components are shown as connected or embedded as part of a bracelet strap.



CONFIDENTIAL

Figure 2. RFID circuitry mounted within the dielectric material of the microstrip antenna. Figure 2 shows the Radio frequency identification (RFID) components mounted in the dielectric on the bottom of the top plate, on top of the ground plane, or in between. Using bare die components allows the use of circuit elements as thin as 10 to 20 mils in height.

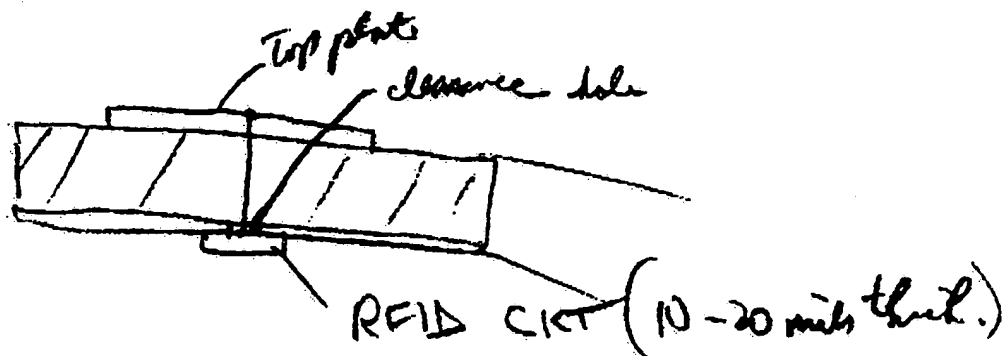


Figure 3. RFID circuitry mounted on the underside of the microstrip antenna. Figure 3 shows the Radio frequency identification (RFID) components mounted on the underside of the ground plane. Using bare die components allows the use of circuit elements as thin as 10 to 20 mils in height.

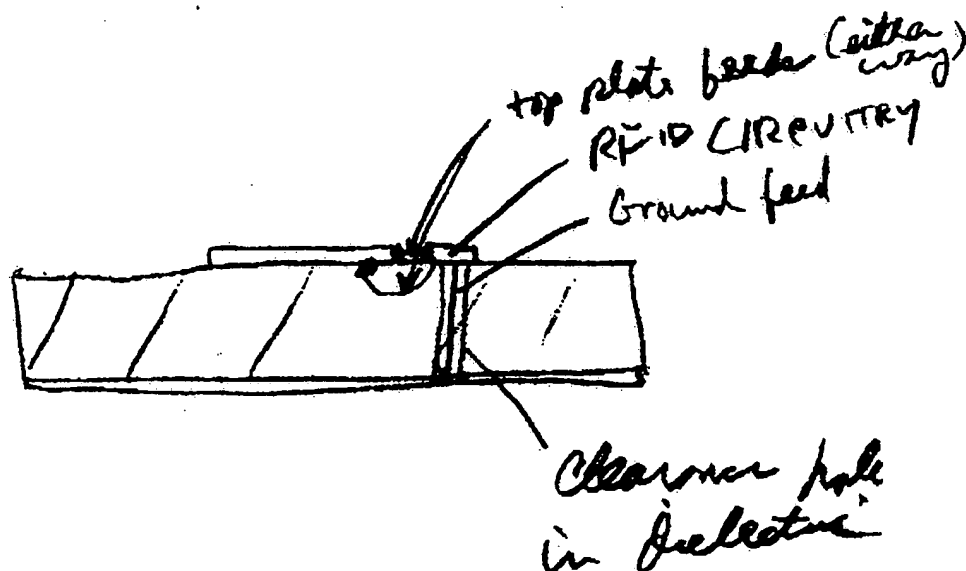


Figure 4. RFID circuitry mounted next to the top plate. Figure 4 shows the RFID circuitry mounted on top of the dielectric, next to the top plate. A hole through the dielectric allows the RFID circuit to contact the ground plane under the dielectric.

CONFIDENTIAL

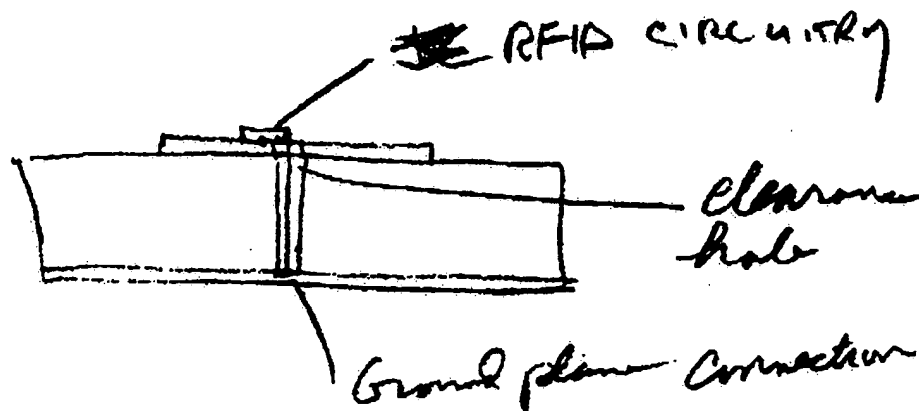


Figure 5. RFID circuitry mounted on top of the top plate. Figure 4 shows the RFID circuitry mounted on top of the dielectric, next to the top plate. A clearance hole through the top plate and the dielectric allows the RFID circuit to contact the ground plane under the dielectric.

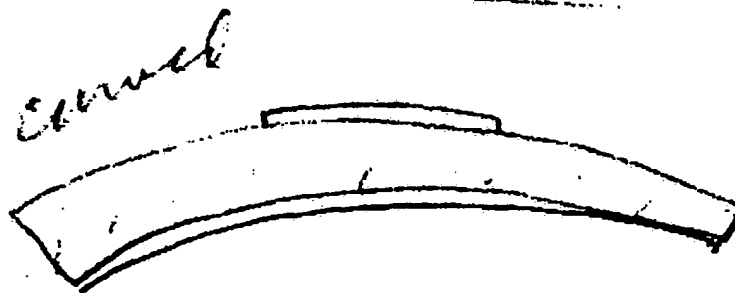


Figure 6. A curved microstrip antenna. Figure 6 shows a curved microstrip antenna, allowing a better fit to the patient. A bracelet may be attached to the antenna and circuitry as shown in figure 1.

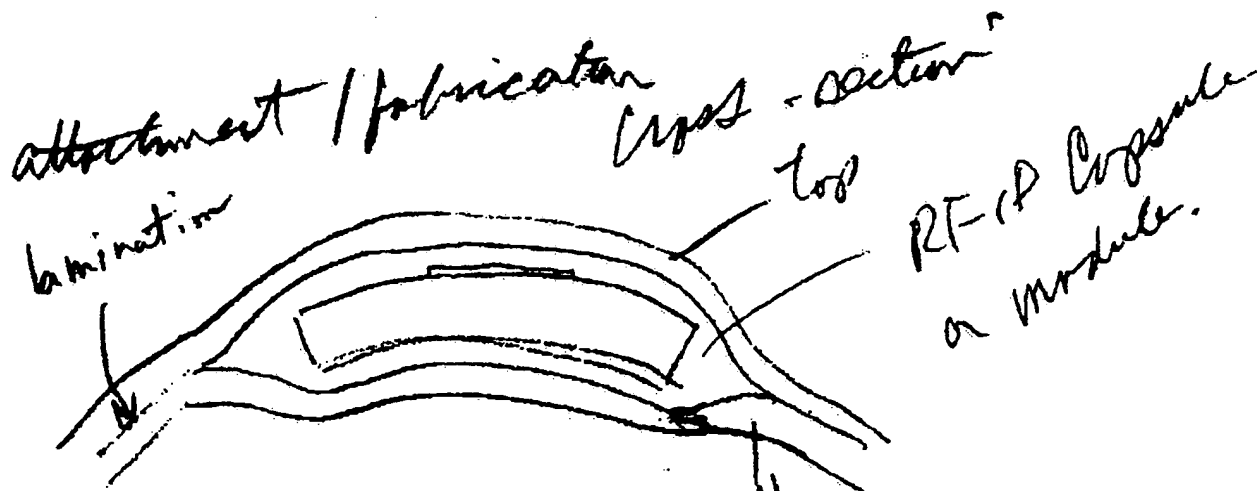


Figure 7. Method of attaching the bracelet to the antenna and RFID circuitry. Figure 7 shows the antenna and circuitry laminated in between top and bottom non-conducting layers of bracelet material. The embedded Antenna and circuit module are made beforehand or at the time of fabrication of the wristband product.

**FIGURE 8 AND SUBSEQUENT TO BE ADDED BY MB. PATCH ANTENNA ELEMENTS
IN SECUREMENT**

Tuttle: Wristband Patch Antenna
13 June 2001
Page 13

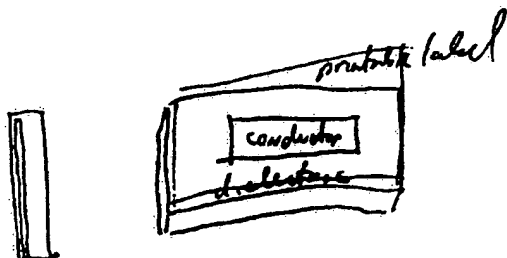
CONFIDENTIAL

APPARATUS.

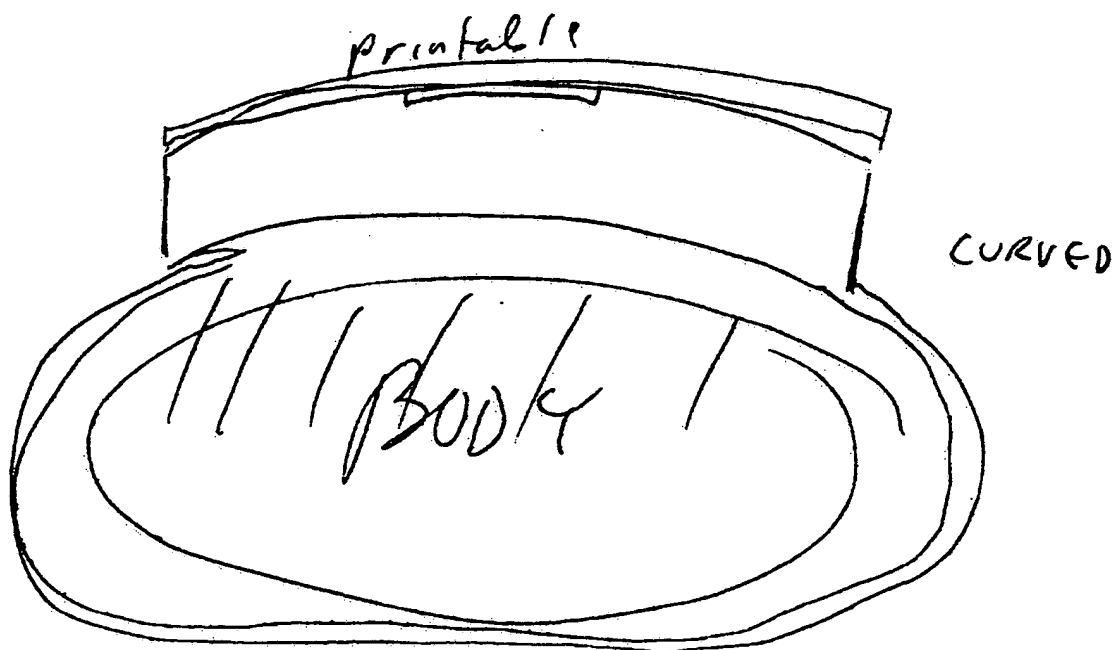
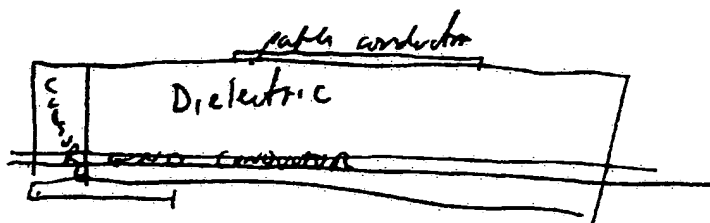
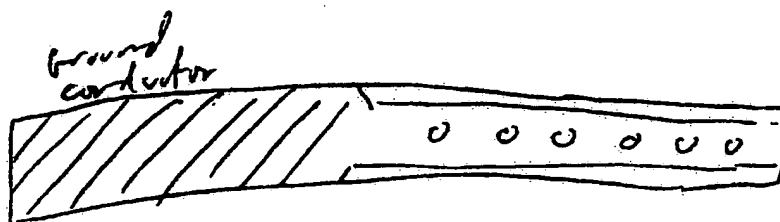
CONFIDENTIAL

6/13/01

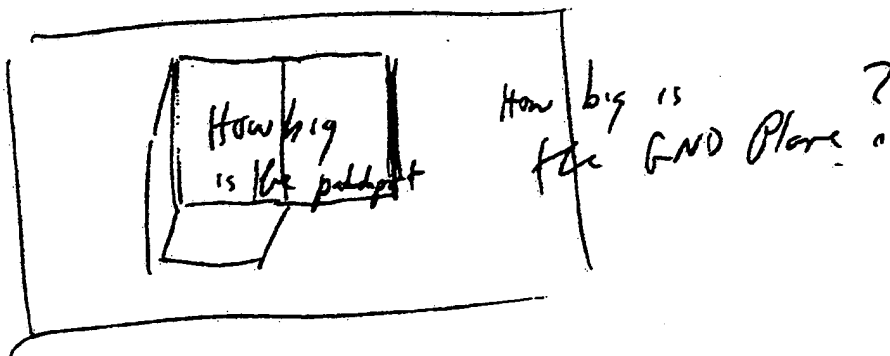
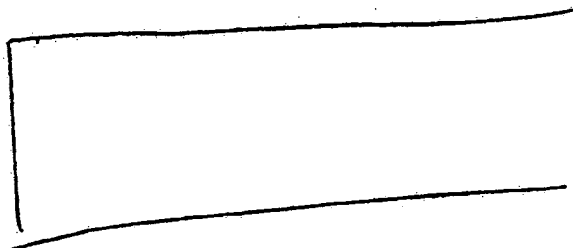
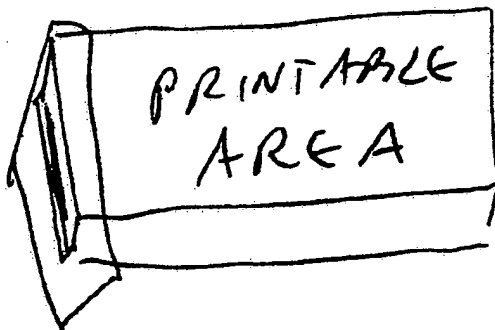
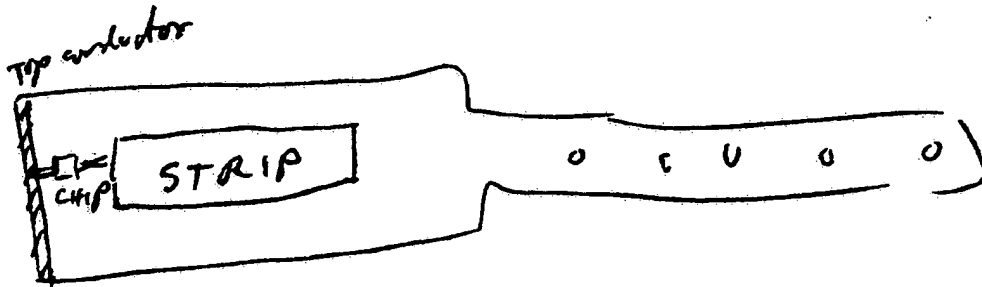
MG



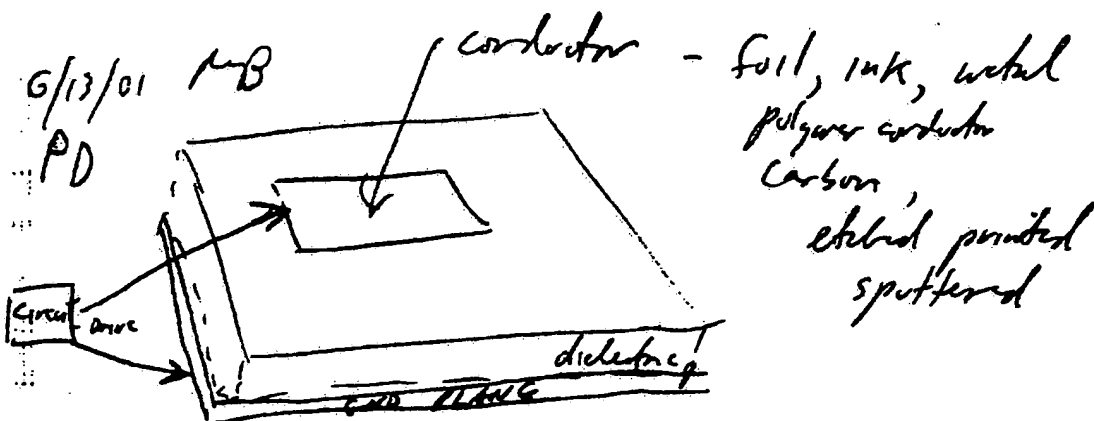
FLAT



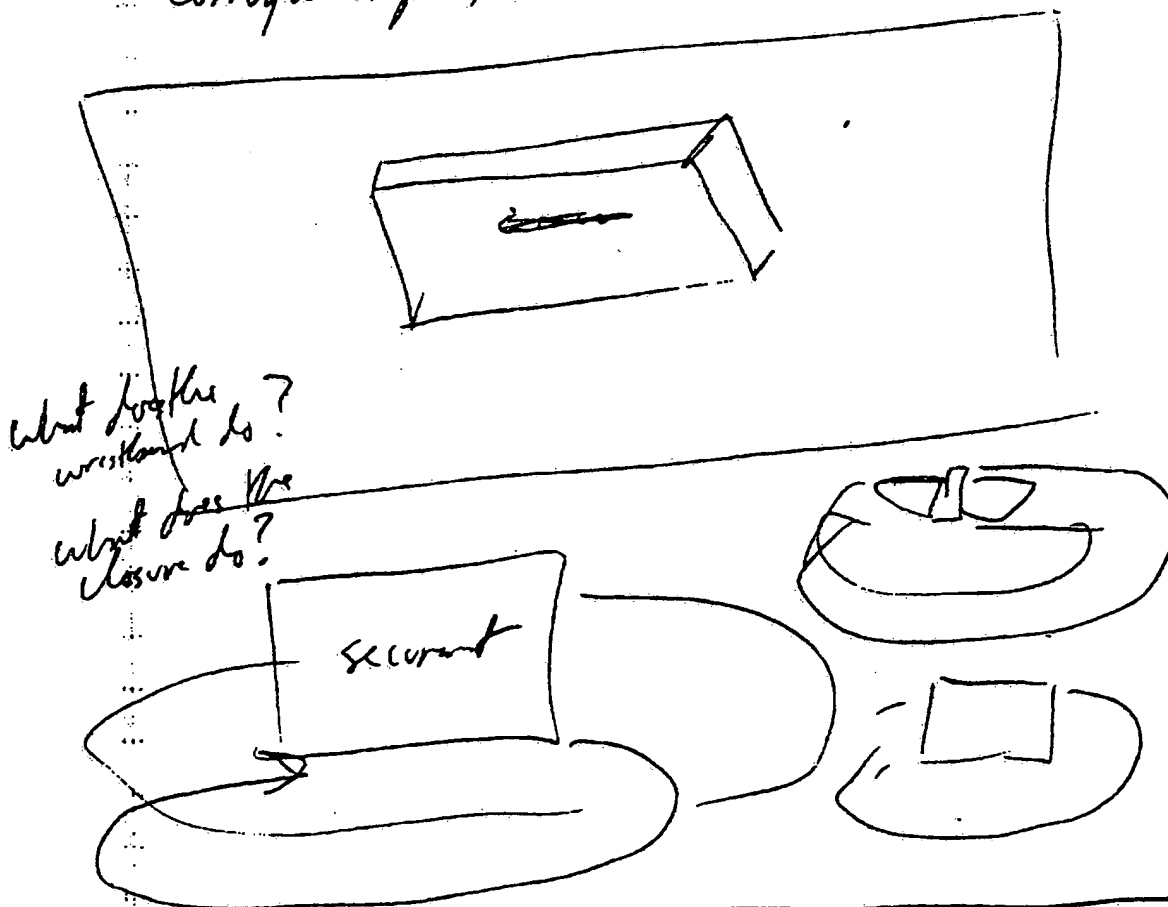
CONFIDENTIAL



CONFIDENTIAL



- Dielectric
- foam
 - plastic
 - air
 - Corrugated plastic



7-2-01

Maybe put foam strip
 under side wristband

Wristband
 FOAM
 SKIN

Revised report section

Subject: Revised report section

Date: Mon, 17 Sep 2001 11:53: -0700

From: "Mike Beigel" <beigel@beitec.com>

To: "Ozzie Penuela" <ozzie@pdcorp.com>

CC: "Walter Mosher" <wwm@pdcorp.com>, "James Geriak" <jwgeriak@lyonlyon.com>,

"Tom Mahoney" <tpmpatlaw@hotmail.com>


CONFIDENTIAL

Enclosed is a revision of section 4 (Invention ideas November 1996) from the report INVENTION EFFORTS SUMMARY distributed at our meeting at PD on September 10, 2001. It is a Microsoft Word file

Tom Mahoney and I met to review this section in for clarification, on September 14, 2001.

The document is printed in black and red, so if you have any problems printing it this was please inform me and I will send you a paper copy.

Mike Beigel

| | |
|---|--|
|  PD Inventions2001REV4.doc | Name: PD Inventions2001REV4.doc Type: Microsoft Word Document (application/msword) Encoding: base64 |
|---|--|



RFID PROJECT FOR PRECISION DYNAMICS CORPORATION

INVENTION EFFORTS SUMMARY

**REVISION OF SECTION 4
(Invention ideas November 11, 1996)**

ALL COMMENTS AND REVISIONS IN RED

ALL PAGES CONFIDENTIAL MATERIAL

Prepared for: Precision Dynamics Corporation

By: Michael L. Beigel Beigel Technology Corp.

Date: August 28, 2001 Revision September 6, 2001

REVISION OF SECTION 4: September 17, 2001

SUMMARY:

This is a revision of section 4 of the draft document: (Invention idea list from November 11, 1996 reports) (For reference)

Tom Mahoney and Mike Beigel met on September 14, 2001 to review section 4 of the document in light of patent applications and issued patents applied for since the date of the idea disclosures.

We reviewed the original list of invention ideas to more clearly describe which of the descriptions developed into subsequent patent disclosures and claims.

This text is issued September 17, 2001.



**BEIGEL
TECHNOLOGY
CORPORATION**

www.beitac.com

• PHONE: (760) 633-3888
• FAX: (760) 633-3819
• E-MAIL: beigel@beitac.com

308 VIA JULITA • ENCINITAS, CA 92024

4: INVENTION IDEAS FROM 1996 PROJECT DOCUMENT: (EDITED 2001)

From

RFID Technology in Identification Wristbands And Flexible Labels

Draft #: 04

Date: November 11, 1996 EDITED: M. BEIGEL AUG 31, 2001

REVISIONS IN RED BY TOM MAHONEY AND MIKE BEIGEL September 14, 2001.

GROUP I: Flexible Disposable RFID Tag for Wristband

1. Laminated Lumped Transponder Antenna on flexible substrate, and Manufacturing process

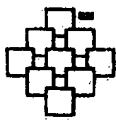
Inductive and capacitive elements of antenna structures for RFID transmissions are printed or stamped on one or both sides of one or more layers of flexible material in the manufacturing process for a wristband or flexible label. Continuous flow processing of (plastic) sheet material on automatic machine results in complete antenna structure contained in flexible end product. Embodiments for various frequency ranges from 100 KHz to 3 GHz are disclosed.

RESULT: Disclosed and claimed in "600" patent, also disclosed and claimed "598" patent.

2. RF antenna on flexible substrate, multi-layer capacitive and inductive coupling

Structures or patterns of conductive material printed on flexible sheets of insulating dielectric material form inductors and/or capacitors. Inductive and/or capacitive coupling between structures on different layers of material form a resonant multi-element antenna circuit without any electrical (ohmic) connection between the elements on the different layers. Possible capacitive coupling to (silicon) IC chip structure affixed to one of the layers of sheet material form a complete ID tag wristband or flexible RFID label.

RESULT: Disclosed and claimed in "600" patent, also disclosed and claimed "287" patent.



3. RFID tag on polymer substrate, with passive components only

An RFID tag made with passive elements (inductors, capacitors, resistors, electrical contacts) is imprinted on one or more layers of flexible material. Possible embodiments are multiple resonant circuits or delay lines. Programming of information on the tag is performed by opening or closing circuits on the tag according to a programming method, resulting in unique coding of each tag up to the number of combinations of open or closed circuits.

RESULT: Disclosed and claimed in "598" patent.

4. RFID tag characterized by programmable multiple delay lines

A high-frequency RFID tag is characterized by a plurality of delay lines, each of which can be switched in or out of the circuit by a programming method. In response to an electromagnetic impulse radiated to the tag by a reader, the tag outputs a sequence of reflected pulses based on the number and length of delay lines connected to a reflective antenna or antennas on the tag, the sequence of pulses determined by the programming of the delay lines.

RESULT: Disclosed in "600" patent disclosure, but not claimed.

5. RFID tag characterized by spectral response to an interrogating signal

An RFID tag characterized by a unique spectral response to an interrogating signal. The tag is programmable to produce a unique set of frequency components in response to the interrogating signal. The interrogating signal can be an impulse, a swept frequency, a waveform having multiple frequency components or a series of stepped frequencies. The tag can be either active (battery powered), passive with active components (in which operating power is derived from the signal coming from the reader and active circuitry is employed in the tag), or purely passive (in which passive resonant circuits or delay lines are used).

RESULT: Not disclosed.

6. Attachment of Integrated circuit ID tag to flexible substrate antenna

An integrated circuit RFID tag is attached to a flexible antenna in a continuous manufacturing process. The attachment may be by capacitive, inductive or ohmic coupling. Means for placing and securing the IC onto the flexible substrate may include ultrasonic bonding, conductive adhesive, UV curing adhesive, or laser welding. Production process and machinery are disclosed.



**BEIGEL
TECHNOLOGY
CORPORATION**

www.beitec.com

• PHONE: (760) 633-3868
• FAX: (760) 633-3819
• E-MAIL: beigel@beitec.com

308 VIA JULITA • ENCINITAS, CA 92024

RESULT: Disclosed and claimed in "287" patent.

7. RFID and Printed Information on flexible ID tag

An RFID tag code as well as printed information are programmed onto a flexible tag. The printed information may be readable text, bar code, photographic print or other. The RFID tag may be programmed at the factory or at the time of deployment. Information contained in the RFID tag may be read by an RFID reader at the time of printing the printed information and used in formulating the information to be printed.

RESULT: Disclosed in "600" patent, Orocio patent?

8. RFID data programmed by printing with conductive ink on a contact matrix

RFID data are programmed onto a flexible RFID tag by printing a pattern of conductive ink marks onto a contact matrix electrically connected to multiple terminals of an RFID tag. The RFID circuit may be either an IC chip, polymer semiconductor structure, or printed passive structure. The printed pattern may be applied either at the factory or at the place of deployment. Additional printed information may be put on the tag at the same time (bar code, readable characters, photographic information, etc.). A device for printing the information on the tag in manufacturing or deployment environment is disclosed.

RESULT: Disclosed and claimed in "598" patent

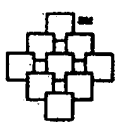
9. RFID tag made with polymer semiconductors on a flexible substrate

A complete RFID tag using polymer based active circuitry is deposited onto one or more layers of flexible material. The tag includes energy receiving element (antenna); information transmitting element (antenna); and active circuitry for deriving operating power (and possibly clock signal) from the energy receiving element, reading an ID code programmed into the circuit, and outputting the ID information to the information transmitting antenna. Enabling disclosure for polymer semiconductors, and fabrication method must be obtained.

RESULT: Disclosed and claimed in "598" patent, disclosed and claimed in "600" patent.

10. Flexible RFID Tag with electromagnetic energy absorption means and optical information transmission means (LED)

The tag is energized by an electromagnetic field signal. The information programmed in the tag is transmitted optically by a polymer LED.



RESULT: Not disclosed.

11. Flexible ID tag with visual readout activated by external electromagnetic field signal

An electromagnetic signal provides power and enabling information to a flexible tag with an LCD readout. Upon energizing and validation signal, the (wristband) displays optically readable output according to information programmed in the tag or received from the interrogating/enabling device.

RESULT: Not disclosed.

GROUP II: Disposable Wristband, Re-usable RFID Tag

12. Disposable wristband and re-usable RFID transponder (Penuela patent 5,493,805)

In place of a button memory in Penuela 5,493,805, an RFID tag is included. Since the RFID tag does not require physical or electronic contact to transfer information, additional embodiments appropriate to secure, sterile containment of the RFID tag should be disclosed. Different types and shapes of RFID tag should be disclosed. Capacitive or inductive coupling to an antenna fabricated on the disposable wristband should be disclosed.

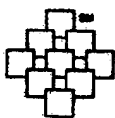
RESULT: This concept matured into Patent application Docket #P5366 "Disposable Reusable"

13. Extension of Soft-Guard Patent

Closure device for Soft Guard wristband augmented to include an RFID tag. Capacitively or inductively coupled antenna installed or printed on inside of wristband tube.

Embodiments consist of:

1. Self-contained RFID tag embedded in wristband closure
2. RFID tag in wristband closure capacitively coupled (or inductively) on one side to fixed-length conductive strip antenna in wristband body
3. RFID tag in wristband enclosure capacitively or inductively coupled on opposite sides to continuous conductive strip antenna in wristband body, forming loop antenna
4. RFID tag in wristband enclosure capacitively or inductively coupled on one side, with two parallel adjacent capacitive or inductive areas, to a fixed length loop antenna embedded in a portion of the wristband body.



5. Re-usable RFID tag removably mounted onto a disposable ID wristband.
6. Removable, re-usable ID wristband with RFID tag. Used like a watch, or in conjunction with a watch. Or an RFID tag in an expensive ornamental wristband such as a piece of jewelry.

RESULT: This concept matured into patent application Docket #P5366 "Disposable/Reusable" Items 1 and 5 are disclosed.

GROUP III: Closure of Wristband Activates RFID Tag

14. Wristband RFID antenna activated by closure of wristband

Operation of RFID tag in flexible wristband is enabled by closure of wristband, as security feature. Enabling may be accomplished by: connecting an antenna, providing power to RFID tag, tuning an antenna, changing the state of a logic input to the tag logic. Enabled tag verifiable by: operation or non-operation, changed code based on logic input.

RESULT: Portions are in patent application Docket #P5366 "Disposable/Reusable".

15. Conductive adhesive wristband closure activates RFID tag (Mosher patent 5,457,906)

Adhesive closure of wristband is augmented by using conductive adhesive to close an electrical circuit, thereby activating RFID function.

RESULT: Conductive adhesive not disclosed.

19. Closure mechanism (Peterson patent 5,479,797) activates RFID wristband

The closure mechanism of Peterson's patent is augmented to enable or activate an RFID tag wristband when closed, and to disable operation if attempted to open. Wristband may contain integral antenna and/or RFID tag disposable or replaceable. Inside of closure mechanism may be coated with conductive material to complete an electrical circuit when engaged.



RESULT: Not disclosed

GROUP IV: Adjustable Wristband Antenna, Constant Resonant Frequency

20. Adjustable RFID wristband antenna with constant resonant frequency

When a wristband RFID tag is adjusted to fit different sizes, the integral antenna maintains a constant resonant frequency, for optimum energy and information transfer. Enabling means must still be discovered.

RESULT: Not disclosed.

GROUP V: Programming RFID Tag, Systems & Database Management

21. Programming RFID wristband at IC fab, wristband factory, end user location

An RFID tag may be programmed with several types of unique or generic information. Depending on the technology used to implement the tag, programming at the IC fab, wristband factory, end user location, or combination of these may be appropriate.

RESULT: Disclosed but not claimed in "598" patent.

22. Identification and database management using wristband, RFID, RFDC

The information contained in an RFID tag is integrated into a complete database management system appropriate to the requirements for managing the identified population. The RFID tag may contain permanent information programmed at the factory not alterable by any means, permanent information programmed at the application site, and alterable information

RESULT: Not disclosed.

23. Patient ID system and database manager for hospitals, using RFID

RESULT: Not disclosed.

GROUP VI: Reader Antenna Systems

24. Doorway RFID Reader Antenna



Reader antenna for low or mid frequency RFID system is disposed on both sides of a doorway. No conductors are disposed along the floor. The configuration on both sides of the doorway creates a more complex E-M field pattern, enhancing reading percentage. A connector or connectors through the wall between the coils provides electrical connection of the E-M structure.

RESULT: Not disclosed.

25. RFID Wristband Uses Human Body As Part of Antenna System

November 4, 1996 Michael Beigel, Isidor Straus

SUMMARY: At certain RF frequencies there is significant electromagnetic coupling between the human body and an RF antenna in close proximity. This effect varies with RF frequency. This effect can be used to enhance the communication efficiency between an RFID wristband and reader-energizer. Since the wristband encircles the wrist (or other part) of the wearer's body, the wristband may embody an RF antenna either adjacent to or completely encircling the wearer's limb. This can be the basis for an optimized antenna design which relies on the predictable proximity to the human body. By choosing an optimum RF frequency based on the construction of the wristband antenna and the average E-M coupling to the wearer's body, the effective communication range or the RFID system can be increased compared to a design which does not utilize this E-M coupling effect and optimize it in the design of the RFID system.

RESULT: Not disclosed.

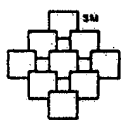
26. Adhesive RFID patch for humans

November 9, 1996 Michael Beigel

A flexible RFID tag, in the shape of a patch, adhered to a removable flexible adhesive medium similar to a "band-aid", can be used for temporarily identifying people in environments or situations in which an RFID wristband would be inappropriate or hazardous. The product would also include protective material easily removable from the adhesive area of the patch, to enable easy storage of multiple tags as well as easy preparation of the patch for attachment.

RESULT: Not disclosed. Believed shown in prior art.

END OF TEXT



**BEIGEL
TECHNOLOGY
CORPORATION**

www.beitec.com

DISCLOSURE

• PHONE: (760) 633-3868
• FAX: (760) 633-3819
• E-MAIL: beigel@beitec.com

308 VIA JULITA • ENCINITAS, CA 92024

RFID PROJECT

11-1-01 Distribution

FOR PRECISION DYNAMICS CORPORATION

W. Mosher
O. Penuela
S. Chaoui

PROJECT PRIORITIES FOR NEW TECHNOLOGY AND INVENTION DEVELOPMENT

ALL PAGES CONFIDENTIAL MATERIAL

Prepared for: Precision Dynamics Corporation
By: Michael L. Beigel Beigel Technology Corp.
Date: October 16, 2001 REVISION: October 31, 2001
FILENAME: ProjectPriorities2.doc

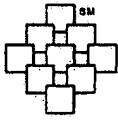
SUMMARY:

This report summarizes and prioritizes technology search, development and invention efforts and ideas for Precision Dynamics RFID, RFID wristband and polymer/flexible electronic technology projects.

1. Current BTC "to do" list
2. Summary of Precision Dynamics R&D interests related to RFID
3. Current patent disclosures and areas of focus
4. Invention idea list 2001
5. Ideas from 1996 disclosures

OBJECTIVES:

Improve the performance and reduce the price of RFID wristbands
Provide RFID function on other PD product lines
Provide reader and printer products to complement the tags
Apply for specific patent coverage on products entering the marketplace
Provide system development assistance to customers
Continue patent development on printable RFID
Investigate emerging technologies
Form alliances with companies and universities



1. Current BTC "To Do" List

This is a summary of all task items currently assigned to BTC or under discussion. The items are prioritized with asterisks (=High, *=Medium, *=Low) according to MB rating of urgency or importance. These should be reviewed with PD as soon as possible to authorize implementation.**

***** Patenting: Invention Disclosures:** Increase PD's intellectual property in areas connected with remote identification of wristbands and other mass-produced ID products.

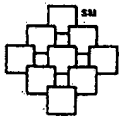
Printable RFID on flexible substrate
Secure RFID wristband
Wristband with RFID and biometrics
Wristband airline ticket
Wristband with display
Di-Cap inventions
Bluetooth Wristband
Patch antenna wristband
Other invention ideas from BTC 1996 document
PD internal invention disclosures

**** Patenting: Research, Licensing and Enforcement:** Find patents PD should be aware of, pursue mutual arrangements with potential business allies, pursue enforcement against infringers.

Nagra
Alien
MIT Licensing Office
UCLA Licensing Office
RFID patent search updates

**** Company and Research Institution Investigation:** Stay up to date with the leading companies in the field, and their technological progress.

Alien Technology
Wave ID
E-ink
MIT Auto-ID center
Digital Angel
UCLA
Philips
NASA



***** Reduction to Practice:** Continue efforts to provide new-technology "breakthrough" implementations for PD RFID products.

Di-Cap

High-speed printable diode
RFID on flexible substrate
Printable memory
RFID with flexible battery

**** Other Project Areas:** Support PD with technology related information to support internal R&D, manufacturing and marketing of RFID product line.

RFID standards

Supply sources for RFID readers, printer/programmers, software/systems
Obtaining government grants
Expanding PD RFID market areas
PD brainstorming meeting
Business arrangements with UCLA, Yang Yang
Other Yang projects

***** Budget:** Formulate realistic budgets to generate project priorities and spending policies for external efforts.

PDC: Internal R&D efforts

BTC: External technology development and research projects
Yang Yang : Organic semiconductor projects
UCLA: Implementation of organic semiconductor projects
Legal (IP): Patenting and IP legal issues
Other: Any other external efforts

People and Resources (BTC): Areas of expertise BTC can supply for PD projects

Mike Beigel: Project management, invention, technology development
Isidor Straus: Electromagnetic interference and compliance
John R. Tuttle: UHF RFID and invention
Barry Blesser: MIT connection and advanced thinking
H. Clark Bell: High frequency issues, patent disclosure writing
Stan Humphries: Electromagnetic field modeling
Nat Polish: Computer science and software design

2. SUMMARY OF Precision Dynamics RFID Research and Development PRESENT R&D INTERESTS

BASIC QUESTIONS

In proposing an invention and IP strategy for Precision Dynamics RFID development work, the following questions provide a framework for specific development and patenting efforts:

What are PD's:

-Present business/technology/market positions?

-Business/technology/market goals for 5-10 years?

What new external technology developments will impact these fields?

What should PD be inventing to promote progress towards its goals?

These questions should be discussed and answered by the group responsible for R&D and intellectual property generation.

AREAS OF R&D WORK FOR BTC

The following are topics of continuing R&D work and patenting as of spring 2001, assigned to BTC:

PRINTABLE SEMICONDUCTOR RFID: Continue towards a prototype RFID on flexible substrate made without silicon chips.

PROJECTS WITH YANG YANG

Continue development towards printable RFID wristbands.

Research and prototype "Di-Cap" Rectifying Charge Storage Element

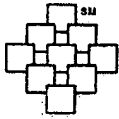
High-speed diode

Proposal for NSF for RFID integrated polymer circuit

OTHER PROJECTS

Find and make contact with other resources for "printable" electronics

HIGH FREQUENCY RFID: Develop technology in 800-915 MHz range and 2.4 GHz (Bluetooth protocol).



Patent application "patch antenna" with John Tuttle
Patent application "Bluetooth wristband" with John Tuttle.

Evaluate current and prospective product offerings for high frequency.

RFID INTELLECTUAL PROPERTY: Advance PD's position re enabling patents for RFID leadership and strategic strength.

Philips patent matter: Re-issue application has been filed
Licensing other patents useful to PD's RFID goals
Continue patent search and analysis in areas of interest
Continue patenting inventions

EMERGING TECHNOLOGIES: Continue to study all emerging technology potentially applicable to remote detection of ID wristbands. Apply for early patents as appropriate.

Areas of inquiry: Ultra-wideband, Nanotechnology, Molecular technology, Printable circuits, Biotechnology, Quantum electronics, self-assembly, 3-D self-assembly, virtual antenna, etc.

Search all other topics that generate technology or science "buzz words" potentially applicable to remote identification systems.

INDUSTRY ALLIANCES: Investigate alliances with companies and universities

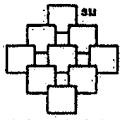
Alien: Investigative report has been completed

UCLA: Form a relationship regarding working with YY

MIT: Approach licensing department
Philips

RFID STANDARDS: Continue to study and inform PD regarding RFID or electromagnetic communication, electromagnetic location standards that may affect business possibilities.

Meet with PD to review first Standards report
Determine next activities
Continue Standards analysis



3. CURRENT PATENT DISCLOSURES RELATING TO BTC PROJECTS

The following patent applications are currently in process:

RFID tag on flexible substrate: Patent issued US 5,973,598 Beigel

Reissue/interference action in process. *7/1/02*

Audio Identification Device Having Reusable Transponder: Patent application in appeal

Mosher, Mahoney, Beigel TM Docket #: PRECI-P5366

Patent claims in appeal

Audio Rectifying Charge Storage Element: Patent filed November 2000

Beigel, Yang TM Docket #: PRECI-P5534 *C-2*

Awaiting first office action US

The following ideas have been submitted to PD as disclosures, and are awaiting evaluation whether to proceed to patent application filing:

RFID Wristband with patch antenna: Disclosure submitted to PD June 2001

Tuttle, Beigel, Bell

RFID wristband with Bluetooth interface: Preliminary disclosure submitted to PD

Tuttle, Beigel Updated disclosure submitted September 6, 2001

Continuation of RCSE (Di-Cap) patent: Notes for disclosure submitted to PD

Beigel, Yang

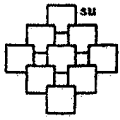
The following ideas have been submitted to PD as disclosures since the last report, and are awaiting evaluation whether to proceed to patent application filing:

Wristband Airline Ticket: Using a wristband as an airline ticket or boarding pass in conjunction with other supporting RFID, security and database attributes

Secure RFID Wristband: Means to prevent and indicate tampering with an RFID wristband

Wristband with Optoelectronic Elements: Using electronics to add display, signaling, power conversion functions to flexible disposable wristbands

Wristband with RFID and Biometric Data: Combining biometric data and RFID technology and wristband inventions.



4: INVENTION IDEA LIST 2001

This is a brief summary of ideas and directions for near term, medium term and long term new invention descriptions and patent applications. It has not been developed. By brainstorming the concepts, many specific invention disclosures may be produced.

PD MAIN OBJECTIVES

1. Minimum cost disposable "RF" wristband with read/write memory, high reliability, high security
2. Easy programming and issuing wristband to user, putting data in database, updating data
3. Increasing the functionality of RFID wristbands

PD WRISTBAND AREAS

1. Hospital/Healthcare
2. Crowd control/Entertainment
3. Law Enforcement

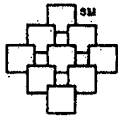
OTHER PD TECHNOLOGY AND PRODUCT AREAS

1. Tickets and labels
2. UV admission
3. Drinkware
4. Pass holder
5. Blood recipient system
6. Urology accessories
7. Labor/Delivery
8. Infection control
9. Patient comfort
10. Fluorescent reference standards
11. Other

Example: Wristband that emits visible light in reader field

INVENTION CLASSES (example)

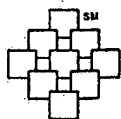
1. Component
2. Circuit



3. Product
4. Tag
5. Reader
6. System
7. Data

PARTIAL LIST OF CONCEPTS AND TECHNOLOGY BUZZ WORDS

RFID
Identification
ID
Short Range Dedicated Communication
SRDC
Flexible Substrate
Wristband
Bracelet
Label
Ticket
Display
Flexible battery
Ultra-wideband
Nanotubes
Nanotechnology
Nanocrystal
Micromachines
Organic Semiconductor
Organic Transistor
Organic Diode
Organic Field Effect Transistor
Organic IC
Organic Sensor
Organic Conductor
Organic Integrated Circuit
Organic Memory
Polymer Integrated Circuit
Polymer Memory
Polymer IC
Polymer Semiconductor
Polymer Field Effect Transistor
Polymer Sensor
Polymer Transistor
Polymer Diode
Doped Polymer
Printable Electronics

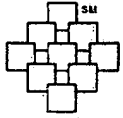


Printable diode
Printable transistor
Printable FET
Printed
OLED
Metallic DNA
Thin Film Transistor
Bluetooth
Biometric
Fingerprint
Iris scan
Voiceprint
DNA print
Face recognition
Data compression
Matching algorithm
Electrophoretic display
Light emitting polymer
Fullerene, buckyball, C60
Flexible display

BIG INVENTIONS: Generic ideas that will enable major technology segments and new markets, development time frame up to 20 years. Speculative: technology may or may not prove feasible, marketable or economic.

Example: Disposable printable GPS wristband with ID, database and biological sensor

SMALL INVENTIONS: Specific ideas that will protect technology/market positions in present technology segments, development time frame 2 to 5 years. Conservative: technology and markets already exist; invention will likely be produced and marketed.



5: INVENTION IDEAS FROM 1996 PROJECT DOCUMENT: SELECTED FOR PRESENT POTENTIAL

NOTE: These ideas were disclosed in 1996:

RFID Technology in Identification Wristbands And Flexible Labels

Draft #: 04

Date: November 11, 1996 EDITED: M. BEIGEL October 17, 2001

The ideas have not been disclosed in Precision Dynamics patent applications. The ideas that still have potential use in patents are listed. These ideas must be compared with currently published patents, patent applications and other published prior art to determine whether to include them in future PD patent applications.

5. RFID tag characterized by spectral response to an interrogating signal

An RFID tag characterized by a unique spectral response to an interrogating signal. The tag is programmable to produce a unique set of frequency components in response to the interrogating signal. The interrogating signal can be an impulse, a swept frequency, a waveform having multiple frequency components or a series of stepped frequencies. The tag can be either active (battery powered), passive with active components (in which operating power is derived from the signal coming from the reader and active circuitry is employed in the tag), or purely passive (in which passive resonant circuits or delay lines are used).

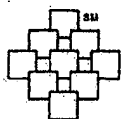
10. Flexible RFID Tag with electromagnetic energy absorption means and optical information transmission means (LED)

The tag is energized by an electromagnetic field signal. The information programmed in the tag is transmitted optically by a polymer LED.

11. Flexible ID tag with visual readout activated by external electromagnetic field signal

An electromagnetic signal provides power and enabling information to a flexible tag with an LCD readout. Upon energizing and validation signal, the (wristband) displays optically readable output according to information programmed in the tag or received from the interrogating/enabling device.

14. Wristband RFID antenna activated by closure of wristband



Operation of RFID tag in flexible wristband is enabled by closure of wristband, as security feature. Enabling may be accomplished by: connecting an antenna, providing power to RFID tag, tuning an antenna, changing the state of a logic input to the tag logic. Enabled tag verifiable by: operation or non-operation, changed code based on logic input.

15. Conductive adhesive wristband closure activates RFID tag (Mosher patent 5,457,906)

Adhesive closure of wristband is augmented by using conductive adhesive to close an electrical circuit, thereby activating RFID function.

19. Closure mechanism (Peterson patent 5,479,797) activates RFID wristband

The closure mechanism of Peterson's patent is augmented to enable or activate an RFID tag wristband when closed, and to disable operation if attempted to open. Wristband may contain integral antenna and/or RFID tag disposable or replaceable. Inside of closure mechanism may be coated with conductive material to complete an electrical circuit when engaged.

21. Programming RFID wristband at IC fab, wristband factory, end user location

An RFID tag may be programmed with several types of unique or generic information. Depending on the technology used to implement the tag, programming at the IC fab, wristband factory, end user location, or combination of these may be appropriate.

22. Identification and database management using wristband, RFID, RFDC

The information contained in an RFID tag is integrated into a complete database management system appropriate to the requirements for managing the identified population. The RFID tag may contain permanent information programmed at the factory not alterable by any means, permanent information programmed at the application site, and alterable information

23. Patient ID system and database manager for hospitals, using RFID

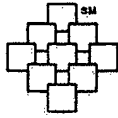
24. Doorway RFID Reader Antenna

Reader antenna for low or mid frequency RFID system is disposed on both sides of a doorway. No conductors are disposed along the floor. The configuration on both sides of the doorway creates a more complex E-M field pattern, enhancing reading percentage. A connector or connectors through the wall between the coils provides electrical connection of the E-M structure.

25. RFID Wristband Uses Human Body As Part of Antenna System

November 4, 1996 Michael Beigel, Isidor Straus

SUMMARY: At certain RF frequencies there is significant electromagnetic coupling between the human body and an RF antenna in close proximity. This effect varies with RF frequency. This effect can be used to enhance the communication efficiency between



an RFID wristband and reader-energizer. Since the wristband encircles the wrist (or other part) of the wearer's body, the wristband may embody an RF antenna either adjacent to or completely encircling the wearer's limb. This can be the basis for an optimized antenna design which relies on the predictable proximity to the human body. By choosing an optimum RF frequency based on the construction of the wristband antenna and the average E-M coupling to the wearer's body, the effective communication range or the RFID system can be increased compared to a design which does not utilize this E-M coupling effect and optimize it in the design of the RFID system.

CONFIDENTIAL

SECURE RADIO FREQUENCY IDENTIFICATION WRISTBAND

Inventors: Michael L. Beigel, Encinitas, CA; H. Clark Bell, Chatsworth, CA

Assignee: Precision Dynamics Corporation, San Fernando, CA

FIELD OF THE INVENTION

This invention relates to wristbands incorporating radio frequency identification (RFID) or other short-range dedicated communications devices, and particularly such wristbands that are made secure and tamperproof.

BACKGROUND OF THE INVENTION

Identification wristbands typically comprise a flexible wrist strap having a length greater than its width, and a closure or securement device for attaching and maintaining the wristband securely around the wearer's wrist. A portion of the wristband is used for imprinting or otherwise attaching the identification or other information regarding the wearer. Various wristband constructions, attachments, and other features are described in U.S. Patent Nos. 6,181,287, 5,973,598, 5,581,924, 5,497,797, 5,493,805, and 5,457,906.

An important aspect of identification wristbands, used for example in hospitals, jails, or hazardous work areas, is security of the information contained in or on the wristband. In order to prevent fraud or mis-identification, it is desirable that the wristband and the associated information be securely and reliably maintained both physically and operationally.

When a wristband incorporates RF communications and data storage functions, opportunities for increased security as well as falsification and fraudulent use are increased.

Of particular importance are the functions of physically securing the wristband to the correct person and insuring tamper detection, the ability of RFID system to transmit a signal, the integrity of the data memory, and the prevention of unauthorized transfer of the RFID and memory devices to another wristband or person.

BRIEF DESCRIPTION OF THE DRAWINGS

DETAILED DESCRIPTION OF THE INVENTION

CONFIDENTIAL

| | | |
|---------------------|--|---------------------------------|
| Los Angeles: | HF Plus, 21111 Tulsa Street, Chatsworth CA 91311-1456 | 818/882-7811 (fax -7815) |
| San Diego: | HF Plus, 321 Sea Ridge Drive, La Jolla CA 92037-7944 | 858/488-4434 (fax -4474) |
| Email: | h.c.bell@ieee.org | |

Descriptions of preferred embodiments of the invention are now described in detail. Referring to the drawings, like numbers indicate like parts throughout the views. As used in the description herein and throughout the claims, the following terms take the meanings explicitly associated herein, unless the context clearly dictates otherwise: the meaning of "a," "an," and "the" includes plural reference; the meaning of "in," alone or in a compound such as "therein," includes "in" and "on"; "radio frequency" and "RF" refer to the frequency range 30 kHz to 300 GHz; "radio frequency identification" and "RFID" refer to identification by radio frequency communication.

The invention is directed to an identification wristband or bracelet, or other attachable appliance, having a flexible substrate carrying an RFID circuit. Application of the invention is not limited to attachment only to the wrist of a person; it can be attached to the wrist or ankle of a person or animal, or to an object. The substrate is an elongated flexible strip of polymer or paper. The RFID circuit includes antenna circuitry, signal generator circuitry, programmable encoder circuitry, and interconnection circuitry. The circuitry comprising the RFID circuit can be, in various combinations, carried in the substrate, or formed by deposition on a layer in the substrate of one or more of conductive paths, semiconductor devices, or polymer materials, in accordance with the '598 patent.

An embodiment of the invention includes a wristband-closing means to securely attach the wristband to a person and circuit-activating means to activate the RFID functions of the circuit at the time of attachment. The wristband-closing means comprises one or more of an adhesive wristband closure in accordance with the '906 patent, a closure mechanism in accordance with the '797 patent, a rivet, or a crimp, which when applied, securely attaches the ends of the wristband to each other, thereby closing the wristband around the wearer's wrist. The circuit-activating means include two or more separate electrical conductors which are connected to the RFID circuit, the conductors comprising one or more of conductive wire or fiber, conductive foil, or a conductor printed on the substrate, and in communication with the conductors one or more of a conductive adhesive, a conductive closure mechanism, a magnetic closure mechanism, a conductive rivet, or a crimp in proximity to the conductors, any of which when applied connects or alters the capacitance between two conductors, thereby closing one or more electrical circuits which may, for example, power the RFID circuit, connect an antenna, tune the antenna, or change a logic state input to the RFID circuit.

Another embodiment of the invention includes circuit-disabling means to inhibit RFID functions of ~~the circuit when the wristband is subjected to tampering or removal from the wearer. The circuit~~ disabling means can include a pattern of electrical interconnections in the substrate, the conductors of which comprise one or more of conductive wire or fiber, conductive foil, or conductors printed on the substrate; when the wristband is stretched or cut, the conductors in the substrate are severed or broken, thereby disconnecting portions of the RFID circuit which may in turn unpower the RFID circuit, disconnect an antenna, detune the antenna, or change a logic state input to the RFID circuit. The circuit-disabling means can also include a pattern of non-conductive fibers in the substrate which are stronger than substrate and electrical interconnections therein; when the wristband is stretched or twisted, the fibers tear the substrate apart and rupture electrical circuits therein, thereby destroying the data carrying device, or the data transmission device, or the entire RFID circuit.

Another embodiment of the invention includes dye-releasing means which releases dye when the wristband is subjected to tampering or removed from the wearer. The dye-releasing means include a dye-filled space in the wristband, and an empty space in the wristband which is adjacent to the dye-filled space; when the wristband is stretched, twisted, or cut, the wall ruptures between the dye-filled space and the adjacent empty space, thereby leaking dye into the empty space and visibly discoloring the wristband, or the wall ruptures between the dye-filled space and the exterior surface of the wristband, thereby leaking dye out of the wristband and discoloring the skin or clothing of the wearer or other person who is tampering with the wristband.

Another embodiment of the invention includes a buckle to adjustably apply the wristband to the wrist and subsequently remove the wristband from the wrist, and a dye tack in communication with the buckle which releases dye when the buckle or dye-tack is subjected to tampering. The buckle is the type which is mounted to one end of the substrate and which when opened, allows free movement of the other end of the substrate through the buckle in order to fit the wristband around the wrist or remove the wristband from the wrist, and when closed, firmly clamps the substrate between movable and fixed portions of the buckle and prevents further movement; the buckle thereby allows the wristband to be applied to or removed from the wrist in a reusable manner. The dye or ink tack is similar to the type used for retail theft deterrence, having locking parts which can be removed intact only with a special tool, and

is attached in such a manner that a portion of the dye tack closes over or around a portion of the closed buckle; ~~when an unauthorized attempt is made to open the buckle or to remove the dye tack from the~~ wristband a dye-filled vial in the dye tack is broken, thereby leaking dye out of the wristband and discoloring the skin or clothing of the wearer or other person who is tampering with the buckle or dye tack.

Another embodiment of the invention includes a buckle as described above, which comprises an electrical conductor, and circuit-activating means to activate said circuit to perform RFID functions upon application of the wristband and to deactivate said circuit upon removal of the wristband. The buckle can be made of an electrically conductive metal of a type which is known to be suitable for buckles, including but not limited to an alloy of iron, copper or aluminum; the buckle can also be made of a polymer having an electrically conductive coating thereon. The circuit-activating means include two separate electrical conductors in the substrate, each of which separately connects to the RFID circuit and extends toward the end of the substrate which does not have the buckle; when the buckle closes and clamps the substrate between movable and fixed portions of the buckle, a direct contact or a capacitive gap forms between each conductor and the buckle conductor, thereby closing an electrical circuit which in turn activates the RFID circuit; when the buckle is opened and the wristband is removed the direct contact or capacitive gap between each conductor and the buckle conductor is removed, thereby opening the electrical circuit which in turn deactivates the RFID circuit.

Although the invention of this application has been described with some particularity by reference to a set of preferred embodiments, it will be readily apparent to those skilled in the art who have reviewed this disclosure that many changes could be made and many apparently different embodiments thus derived without departing from the scope of the invention. Consequently, it is intended that the scope of the invention be interpreted only from the appended claims.

I claim:

1. An identification wristband comprising:
 - (a) an elongated flexible substrate;
 - (b) a radio frequency identification circuit;

(c) wristband-closing means to attach said substrate around the wrist of person to be identified; and

(d) circuit-activating means to enable RFID functions of said circuit upon closure of the wristband.

2. An identification wristband comprising:

- (a) an elongated flexible substrate;
- (b) a radio frequency identification circuit; and
- (c) circuit-disabling means to inhibit RFID functions of said circuit upon tampering with the wristband.

3. An identification wristband comprising:

- (a) an elongated flexible substrate;
- (b) a radio frequency identification circuit; and
- (c) dye-releasing means to release dye upon tampering with the wristband.

4. An identification wristband comprising:

- (a) an elongated flexible substrate;
- (b) a radio frequency identification circuit;
- (c) a buckle to adjustably apply the wristband to the wrist and subsequently remove the wristband from the wrist; and
- (d) a dye tack in communication with said buckle which releases dye when said buckle or dye-tack is subjected to tampering.

5. An identification wristband comprising:

- (a) an elongated flexible substrate;
- (b) a radio frequency identification circuit;
- (c) a buckle to adjustably apply the wristband to the wrist and subsequently remove the wristband from the wrist;
- (d) said buckle comprising an electrical conductor; and
- (e) circuit-activating means to activate said circuit to perform RFID functions upon application of the wristband and to deactivate said circuit upon removal of the wristband..

CONFIDENTIAL

| CLAIM 1 | DESCRIPTION |
|--|---|
| An identification wristband comprising: | The present invention is directed to an identification wristband or bracelet, or other attachable appliance, having a flexible substrate carrying an RFID. |
| (a) an elongated flexible substrate; | The substrate is an elongated flexible strip of polymer or paper. |
| (b) a radio frequency identification circuit; | The RFID circuit includes antenna circuitry, signal generator circuitry, programmable encoder circuitry, and interconnection circuitry. The circuitry comprising the RFID circuit can be, in various combinations, carried on the substrate, carried within the substrate between layers therein, or formed by deposition on one or more layers within the substrate of one or more of conductive paths, semiconductor devices, or polymer materials, in accordance with the '598 patent. |
| (c) wristband-closing means to attach said substrate around the wrist of person to be identified; and | The wristband-closing means comprises one or more of an adhesive wristband closure in accordance with the '906 patent, a closure mechanism in accordance with the '797 patent, a <u>rivet</u> , or a <u>crimp</u> , which when applied, securely attaches the ends of the wristband to each other, thereby closing the wristband around the wearer's wrist. |
| (d) circuit-activating means to activate said circuit to perform RFID functions upon closure of the wristband. | The circuit-activating means include two or more separate electrical conductors which are connected to the RFID circuit, the conductors comprising one or more of conductive wire or fiber, conductive foil, or a conductor printed on the substrate, and in communication with the conductors one or more of a conductive adhesive, a conductive closure mechanism, a <u>magnetic closure mechanism</u> , a <u>conductive rivet</u> , or a <u>crimp in proximity to the conductors</u> , any of which when applied connects or <u>alters the capacitance between two conductors</u> , thereby closing one or more electrical circuits which may, for example, power the RFID circuit, connect an antenna, tune the antenna, or change a logic state input to the RFID circuit. |

CONFIDENTIAL

| CLAIM 2 | DESCRIPTION |
|---|---|
| <p>An identification wristband comprising:</p> <ul style="list-style-type: none">(a) an elongated flexible substrate;(b) a radio frequency identification circuit; and | <p>[Same as in CLAIM 1]</p> |
| <p>(c) circuit-disabling means to inhibit RFID functions of said circuit upon tampering with the wristband.</p> | <p>The circuit-disabling means can include a pattern of electrical interconnections which is embedded within and throughout the substrate, the conductors of which comprise one or more of conductive wire or fiber, conductive foil, or conductors printed on the substrate; when the wristband is stretched or cut, the conductors in the substrate are severed or broken, thereby disconnecting portions of the RFID circuit which may in turn unpower the RFID circuit, disconnect an antenna, detune the antenna, or change a logic state input to the RFID circuit.</p> <p>The circuit-disabling means can also include a pattern of non-conductive fibers, stronger than substrate and electrical interconnections therein, which is embedded within and throughout the substrate; when the wristband is stretched or twisted, the fibers tear the substrate apart and rupture electrical circuits within, thereby destroying the data carrying device, or the data transmission device, or the entire RFID circuit.</p> |

| CLAIM 3 | DESCRIPTION |
|---|--|
| An identification wristband comprising: (a) an elongated flexible substrate; (b) a radio frequency identification circuit; and | [Same as in CLAIM 1] |
| (c) dye-releasing means to release dye upon tampering with the wristband. | The dye-releasing means include a dye-filled space which is embedded within the wristband, and an empty space within the wristband which is adjacent to the dye-filled space; when the wristband is stretched, twisted, or cut, the wall ruptures between the dye-filled space and the adjacent empty space, thereby leaking dye into the empty space and visibly discoloring the wristband, or the wall ruptures between the dye-filled space and the exterior surface of the wristband, thereby leaking dye out of the wristband and discoloring the skin or clothing of the wearer or other person who is tampering with the wristband. |

| CLAIM 4 | DESCRIPTION |
|--|--|
| An identification wristband comprising: (a) an elongated flexible substrate; (b) a radio frequency identification circuit; | [Same as in CLAIM 1] |
| (c) <u>a buckle to adjustably apply said substrate to the wrist and subsequently remove said substrate from the wrist; and</u> | <u>The buckle is the type which is mounted to one end of the substrate and which when opened, allows free movement of the other end of the substrate through the buckle in order to fit the wristband around the wrist or remove the wristband from the wrist, and when closed, firmly clamps the substrate between movable and fixed portions of the buckle and prevents further movement; the buckle thereby allows the wristband to be applied to or removed from the wrist in a reusable manner.</u> |
| (d) <u>a dye tack in communication with said buckle which releases dye when said buckle or dye-tack is subjected to tampering.</u> | <u>The dye or ink tack is similar to the type used for retail theft deterrence, having locking parts which can be removed intact only with a special tool, and is attached in such a manner that a portion of the dye tack closes over or around a portion of the closed buckle; when an unauthorized attempt is made to open the buckle or to remove the dye tack from the wristband a dye-filled vial within the dye tack is broken, thereby leaking dye out of the wristband and discoloring the skin or clothing of the wearer or other person who is tampering with the buckle or dye tack.</u> |

why only buckle

| CLAIM 5 | DESCRIPTION |
|--|--|
| An identification wristband comprising: (a) an elongated flexible substrate; (b) a radio frequency identification circuit; (c) <u>a buckle to adjustably apply the wristband to the wrist and subsequently remove the wristband from the wrist;</u> | [Same as in CLAIM 4] |
| (d) <u>said buckle comprising an electrical conductor; and</u> | <u>The buckle can made of an electrically conductive metal of a type which is known to be suitable for buckles, including but not limited to an alloy of iron, copper or aluminum; the buckle can also be made of a polymer having an electically conductive coating thereon.</u> |
| (d) circuit-activating means to activate said circuit to perform RFID functions upon application of the wristband and to deactivate said circuit upon removal of the wristband. | <u>The circuit-activating means include two separate electrical conductors on or within the substrate, each of which separately connects to the RFID circuit and extends toward the end of the subtrate which does not have the buckle; when the buckle closes and clamps the substrate between movable and fixed portions of the buckle, a direct contact or a capacitive gap forms between each conductor and the buckle conductor, thereby closing an electrical circuit which in turn activates the RFID circuit; when the buckle is opened and the wristband is removed the direct contact or capacitive gap between each conductor and the buckle conductor is removed, thereby opening the electrical circuit which in turn deactivates the RFID circuit.</u> |

| CLAIM 6 | DESCRIPTION |
|--|---|
| A method of attaching an identification wristband comprising the steps of: | |
| (a) crimping or embossing in the wristband a pattern to identify a person or entity by simultaneously | Crimping or embossing in the wristband a pattern to identify a person or entity includes impressing upon the substrate a pattern corresponding to the identity of the person or entity; the pattern can be one or more of an arrangement of figures, symbols or characters, a bar code, or a drawing. |
| (i) closing said wristband around a wrist, | Closing of the wristband includes applying to the overlapping portions of the substrate one or more of the steps of deforming the substrate, rupturing walls of adhesive-filled microspaces in the substrate and curing the adhesive by <u>radio frequency</u> , heat or ultraviolet exposure, or by rupturing walls of microspaces in the substrate separately filled with adhesive and catalyst which mix and cure thereupon. |
| (ii) forming visible means to identify said person or entity, | Forming visible means to identify the person or entity includes one or more of the steps of embossing the pattern, <u>activating pressure sensitive material in the substrate, or colorless adhesive and catalyst becoming colored when mixed or cured.</u> |
| (iii) forming electrical circuits in the wristband corresponding to said pattern; and | |
| (b) storing information in nonvolatile memory in the wristband corresponding to said formed circuits to electronically identify said person or entity. | |

| CLAIM 7 | DESCRIPTION |
|---|-------------|
| A method of attaching an identification wristband comprising the steps of: | |
| (a) crimping or embossing in said wristband a first pattern to identify a first person or entity by simultaneously | |
| (i) closing said wristband around a wrist, and | |
| (ii) forming visible means to identify said first person or entity; | |
| (b) crimping or embossing in said wristband a second pattern to identify a second person or entity by forming electrical circuits in the wristband corresponding to said pattern; | |
| (c) storing information in nonvolatile memory in the wristband corresponding to said formed circuits to electronically identify said second person or entity. | |

Additions by Mike Beigel November 4, 2001 in red:

Closure and securement of band by a crimping or embossing machine with a seal or other pattern identifying the organization or identity of the agent performing the securement process.

Simultaneous programming of RFID information corresponding to the sealer. Microencapsulated adhesive embedded in or on the band, activated by the crimping process. Crimping and heat, ultraviolet curing. Crimping pattern having discontinuities and wristband having a conductive fiber or other conductive pattern, forming a number of circuit connections when crimped, the combination circuit connections being read into a nonvolatile memory in the tag, corresponding to tamper protection reference memory.

Fingerprint data programmed into data memory at time of issuing band. Fingerprint sensor integral to band. Fingerprint sensor integral to band referencing data programmed into memory at issuance of band. Sensor operation only activated in presence of electromagnetic field. Other biometric information similarly entered and checked.

Fingerprint data entered in RFID tag integral to band, at time of issuing band. RFID reader and fingerprint sensor device integrated into "hand tunnel": hand is placed in tunnel (with close range RFID reader) and forefinger placed on fingerprint sensor in tunnel/ (MB will draw diagram). Fingerprint data read by sensor validated against fingerprint data previously entered in RFID memory at issuance.

Subject: Confidential Disclosure

Date: Wed, 12 Dec 2001 11:09:26 -0800

From: "Mike Beigel" <beigel@beitec.com>

To: "Walter Mosher" <wmm@pdcorp.com>

CC: "Ozzie Penuela" <ozzie@pdcorp.com>, "John R. Tuttle" <jrtuttle@sprynet.com>, "David Wang" <dewang@lyonlyon.com>

- CONFIDENTIAL AND PROTECTED BY ATTORNEY-CLIENT PRIVILEGE -

This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.


Dear Walter, Ozzie, John, Clark,

The enclosed confidential disclosure Enhancedwristband1.doc contains the unifying architecture to bring together aspects of the other disclosures we have been working on.

The separate subsidiary disclosures (listed in the main disclosure) are available to each of you as needed.

Please review and send your comments and ideas.

Mike Beigel

| | |
|--|---|
|  Enhancedwristband1.doc | Name: Enhancedwristband1.doc Type: Microsoft Word Document (application/msword) Encoding: base64 |
|--|---|



**BEIGEL
TECHNOLOGY
CORPORATION**

www.beitec.com

• PHONE: (760) 633-3868
• FAX: (760) 633-3819
• E-MAIL: beigel@beitec.com

308 VIA JULITA • ENCINITAS, CA 92024

**PRECISION DYNAMICS CORPORATION
RFID PROJECT**

**ENHANCED ELECTRONIC IDENTIFICATION
WRISTBAND**

ALL PAGES CONFIDENTIAL MATERIAL

Prepared for: Precision Dynamics Corporation
By: Michael L. Beigel Beigel Technology Corp
Date: November 30, 2001 REVISION: December 12, 2001
FILENAME: Enhancedwristband1.doc

DRAFT ONLY: NOT FOR DISTRIBUTION

INVENTORS

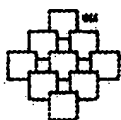
Walter Mosher
Ozzie Penuela
Mike Beigel
John R. Tuttle
H. Clark Bell

(Other PD inventors? Jim Benzman?, Irwin Thal?, Sam Chaoui?)

**SUGGESTION: THIS MATERIAL MAY BE ADDED TO THE
DISCLOSURE "SECURE RFID WRISTBAND"**

**PRECISION DYNAMICS CORPORATION
RFID PROJECT**

ALL PAGES CONFIDENTIAL MATERIAL



SUMMARY:

This disclosure, **ENHANCED ELECTRONIC IDENTIFICATION WRISTBAND**, provides the basis for unification and synergistic combination of the following PD invention disclosures presently under development:

Wristband Patch Antenna:

Disclosure date: June 13, 2001 Tuttle, Beigel, Bell
FILENAME TUTTLE2MB5PATCHDISCL1.doc.)

Bluetooth Wristband

(Disclosure title: "Patient Monitoring System"
Tuttle, Beigel, September 7, 2001
FILENAME: TUTTLEBLU revised3.doc)

Secure Wristband:

MB disclosure Oct 3, 2001
FILENAME: secureRFDIwrist.doc
MB and Clark Bell disclosures Dec.10, 2001
FILENAME: SWBDESCR.DOC
SWBCHART.DOC

Wristband with Biometric Functions:

Mosher, Beigel, Tuttle, Penuela
November 9, 2001 FILENAME: Biometricwristband5.doc

Wristband with Electro-optical components:

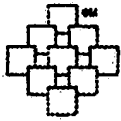
M. Beigel, October 15, 2001
FILENAME: Opticalwristband.doc

Wristband airline ticket:

Beigel October 3, 2001
FILENAME: Airlineticket.doc

Wristband green card:

Oswaldo Penuela MEMO: November 28, 2001
FILENAME: Biometrics for US Dept of State memo.doc



Enhanced Electronic Identification Wristband: Background

Identification wristbands or bracelets have become a convenient and effective way of identifying people without permanently marking them. A principle advantage of a wristband is that it is ultimately removable.

Biometric identification technologies can provide extremely reliable identification of a person.

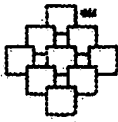
Positive identification of a person and additional data carried by the person (either relating to the person or other types of data including financial transaction data or medical data) may be conjoined by the use of a wristband or similar apparatus that can carry the data, and in addition provide a positive link to the person's intrinsic biometric identification.

However there are situations in which the security of a remotely readable identification device and data carrier require that the device such as a wristband, can only be secured to the person by an authorized person or agency, and once secured to the person being identified, cannot be removed or the data connected with it used except by an authorized party or agency.

Wristbands are advantageous over other forms of ID cards containing data (such as credit cards, tickets or the like), since they can be attached to the bearer physically securely.

Advances in science and technology have provided and will further provide miniaturization of complex electronics; printable electronics including circuitry, memory and power sources; flexible display devices; miniature biometric data analyzers; passive RFID systems, short-range communication networking devices. Specific technologies include self-assembly, Nanotechnology, organic semiconductors, Bluetooth, and others listed in Appendix 1.

Wristbands combining electronic and other technologies to enhance their security and utility, and systems providing data communication between the wristbands, people using the wristbands, communication devices spaced apart from the wristbands, and data management systems are now feasible at a level that can enhance human security, commerce and communication.



Embodiments of the enhanced ID wristband

Version 1: Removable and re-usable wristband, but also capable of being “locked” (physically, biometrically and data) for periods of time, for use in controlled security situations. Not just like a watchband, where you can take it off and put it on anybody else and still have it work. A biometric feature such as a fingerprint enables a biometric sensor on the wristband to correlate wristband with bearer and enable secure “locking” of wristband identity to the person’s identity. A physical locking or tamper indicating mechanism prevents removal or transference of the wristband while in locked mode.

Version 2: Disposable wristband incorporating functions of version 1, except that the fastening means is not re-usable and the functionality of the wristband is destroyed after one use. Various functions of the wristband data archive may be preserved or downloaded after completion of use.

Disposable

Very inexpensive

Version 3: Disposable section, re-usable section: A disposable section (for example the wristband section) and a re-usable section.(for example the RF communication, data storage, data display)

Each version of the wristband embodiments may have components, features and attributes from one to any combination including all elements described in detail below.

INVENTION CLASSES (example)

1. Component
2. Circuit
3. Product
4. Tag
5. Reader
6. System
7. Data

Examples of enhanced ID wristband

RFID function: The wristband may contain an RFID function of any type and frequency, passive, active, low frequency, high frequency, read-only, read-write.

Patch Antenna: The wristband may have a patch antenna (See details from “PATCH” disclosure) and



Networked communication: The wristband may in addition provide network communication using Bluetooth or other wireless protocol (See details from BLUETOOTH disclosure).

Biometric sensor: The wristband may employ one or more biometric sensing devices (Fingerprint, voiceprint, iris scanning, face scanning, body chemical sensing, pulse sensing, and other (Make sure to include a complete list of biometric sensing technologies presently described in prior art)).

Other sensors: Other sensors may be carried by the wristband, having sensing functions other than biometric sensing of data directly related to the bearer of the wristband.

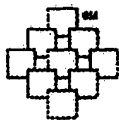
Storage of biometric data: The wristband may store data derived from biometric sensing apparatus on the wristband, or data provided externally to the wristband via a communications interface.

Secure fastening: The wristband may be physically securely fastened such that tampering or removal destroys it function or is rendered evident. The securement may be permanent for the usage life of the wristband, or may be temporary (defeatable by an authorized procedure). In the case of temporary securement, the wristband may be re-used and re-secured by authorized agency.

Securement by data: The equivalent function to physical securement is securement by means of a data structure. The physical securement of the device by authorized agency may cause a data change within the device electronics. Upon unauthorized tampering or removal, a sensor in the wristband may send data to the device or change data in the device, indicating tampering or other breach of security.

Location of Wristband: The wristband may be equipped to provide information about its location. The location information may be provided over a small area (a room or a building) or a large area (countrywide or worldwide), and may be provided with a varying degree of accuracy (less than 1 meter uncertainty to greater than 1 kilometer uncertainty). The location function may be accomplished by calculation derived by the wristband of signals received by it (such as GPS or Local Positioning System), or the location function may be derived externally to the wristband (such as a matrix of RF receivers responding to the signal strength of communications received from the wristband).

Remote read/write of data: Data may be entered into and retrieved from a memory carried on the wristband. The data may be entered and retrieved by means of an electrical connection to the circuitry carried by the wristband, or remotely via an RF communication function of the circuitry. The data may also be communicated via an electro-optical data link, or an acoustical data link.



Opto-electronic components: The wristband may carry optical electronic components or circuits including signaling (light emitting diode), indicating (light emitting or reflectance varying), display (of alphanumeric or image data by pre-formed indicators or matrix of indicators), sensing (of light levels or images), power conversion (photovoltaic cell). These components may be of silicon, polymeric or other materials. They may be inflexible and attached on the wristband or flexible and attached to or printed on the wristband.

Acoustical components: The wristband may carry acoustical components for sensing, communication and indicator functions.

Battery: The wristband may contain a battery to provide primary or auxiliary power for electronic circuitry carried by it. The battery may be replaceable or not. The battery may be a flexible polymer battery imprinted on or constructed on the wristband substrate.

Electronic Article Surveillance: The wristband may contain an electronic article surveillance (EAS) tag in addition to or in combination with its other features.

Dye Sublimation printing: Get details from Jim and Irwin.

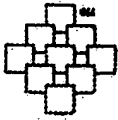
Printed semiconductor: The wristband may electronic components may be either partially or totally constructed from semiconductors, conductors and insulators, which may be inorganic or organic, and which may be printed on the substrate of the wristband. The substrate and the printed components may be flexible.

Flexible keyboard: The wristband may contain a flexible keyboard (symbolic or alphanumeric) for data or password entry directly into the wristband electronics.

Voice Communications: The wristband may have audio transducers for audio input or output, and circuitry of algorithms for processing speech sound and providing two-way speech communication with remote units, and circuitry or algorithms for deriving biometric data from speech sound.

Waterproof: The wristband may be made water resistant, waterproof, and resistant to certain solvents or chemicals used in the area of its application.

Nanotechnology, etc.: The wristband may employ various types of emerging technologies such as (Technology buzz word list) to accomplish the advanced functions, form factor, performance requirements and cost requirements. Enabling documents for these technological areas are included in Appendix 1.



Example applications of the enhanced ID wristband in systems

THESE ITEMS STILL NEED EXPANSION

Airline Ticket and boarding pass, and baggage management (Beigel disclosure)

Green Card (Penuela disclosure)

Hospital Management (Tuttle disclosure)

Amusement Park (PD disclosure)

High Security Facility (Bell disclosure)

Detention Facility (PD disclosure)

What's (the detailed description of)

The wristband?

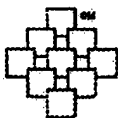
The communication?

The electronics?

The sensors

The information?

The application?



Appendix 1: Technology areas of relevance

The following technical terms relate to public disclosures enabling the inclusion of the related technologies in embodiments of the Enhanced Electronic Identification Wristband

PARTIAL LIST OF CONCEPTS AND TECHNOLOGY TERMS IN CURRENT LITERATURE

RFID
Identification
ID
Short Range Dedicated Communication
SRDC
Flexible Substrate
Wristband
Bracelet
Label
Ticket
Display
Flexible battery
Ultra-wideband
Nanotubes
Nanotechnology
Nanocrystal
Micromachines
Organic Semiconductor
Organic Transistor
Organic Diode
Organic Field Effect Transistor
Organic IC
Organic Sensor
Organic Conductor
Organic Integrated Circuit
Organic Memory
Polymer Integrated Circuit
Polymer Memory
Polymer IC
Polymer Semiconductor
Polymer Field Effect Transistor
Polymer Sensor
Polymer Transistor
Polymer Diode
Doped Polymer



**BEIGEL
TECHNOLOGY
CORPORATION**

www.beitec.com

• PHONE: (760) 633-3868
• FAX: (760) 633-3819
• E-MAIL: beigel@beitec.com

308 VIA JULITA • ENCINITAS, CA 92024

Printable Electronics
Printable diode
Printable transistor
Printable FET
Printed
OLED
Metallic DNA
Thin Film Transistor
Bluetooth
Biometric
Fingerprint
Iris scans
Voiceprint
DNA print
Face recognition
Data compression
Matching algorithm
Electrophoretic display
Light emitting polymer
Fullerene, buckyball, C60
Flexible display
Micromachines

Version I

269/223
PATENT

S P E C I F I C A T I O N
ENHANCED IDENTIFICATION APPLIANCE

FIELD OF THE INVENTION

5 The field of the invention relates generally to identification appliances such as wristbands, and in particular to an identification appliance with a biometric sensor, chemical sensor, optical sensor, heat sensor, pressure sensor, humidity sensor, electromagnetic sensor, acoustic sensor, various opto-electronics and/or various security features such as tamper-evident and tamper-resistant features.

BACKGROUND OF THE INVENTION

10 This disclosure contemplates an improved identification wristband, bracelet, patch, headband, necklace, card, sticker, or other wearable appliance, which for the sake of convenience, are collectively referred to as a "band" or as a "identification appliance". Identification bands have become a convenient and effective way of identifying people
15 without permanently marking them. A principle advantage of a band is that it is ultimately removable. Identification bands typically consist of a flexible wrist strap having a length greater than its width, and a closure or securement device for attaching and maintaining the band securely around the wearer's wrist. A portion of the band may be used for imprinting or otherwise attaching identification or other information
20 regarding the wearer. Bar codes, radio frequency identification (RFID) devices and the like may also be used to store and transfer information associated with the band and the associated person or object. For example, RFID devices includes those which operate in the frequency in the range 30 kilohertz (kHz) to 300 Gigahertz (GHz). Various band

3/1/02

constructions, attachments and other features including the storage of electronic data and RFID functions are described, for example, in Penuela U.S. Patent No. 5,493,805, Mosher U.S. Patent No. 5,457,906, Mosher U.S. Patent No. 5,973,600, Beigel U.S. Patent No. 5,973,598, Beigel U.S. Patent No. 6,181,287, Peterson U.S. Patent No. 5,479,797, and Peterson U.S. Patent No. 5,581,924.

Bands are advantageous over other forms of ID cards containing data (such as credit cards, tickets or the like) since they can be attached to the wearer physically securely. As a result, current uses of identification bands include patient identification in hospitals, clinics and other locations; access in amusement parks; temporary security measures, facility access control, and ticketing and entitlement functions. While identification bands have been used for these purposes, additional applications for identification bands and the like are needed.

One important use for identification bands is patient identification and location in hospitals, clinics and other locations. When used in conjunction with an appropriate reader, patient information can be collected electronically and used by the medical staff in performance of their duties. Another example is to track the location of personnel such as convicts in a prison. When identification bands are used to designate who has authority to enter a restricted area, whether it be a concert hall or prison, the method of attachment of the identification band must be secure. Identification wristbands typically consist of a flexible wrist strap and a closure device for attaching and maintaining the wristband securely around the wearer's wrist. Further, an important aspect of identification bands, used for example in hospitals, jails, or hazardous work areas, is the

security of the information contained in or on the band. In order to prevent fraud or mis-
identification, it is desirable that the band and the associated information be securely and
reliably maintained both physically and operationally. Although the prior art has
attempted to make an identification band more secure, there is a need for further
5 improvements.

Identification bands provide information simply, for example by a person visually
reading printed information on the band, scanning barcode information, or electronically
reading identification information transmitted by the identification band. Thus, barcodes,
RFID devices and the like are used to enhance the information storage and data transfer
10 of information associated with the band and the associated person or object. There is a
need to improve the type of information contained on an identification band as well as the
manner in which the information is maintained.

Moreover, when an identification band incorporates wireless communications and
data storage functions, opportunities for increased security as well as falsification and
15 fraudulent use are increased. Of concern are insuring tamper detection, tamper
prevention, secure transmission of information, the integrity of the information, and the
prevention of unauthorized transfer of the information to others. Improvements in each
of these areas are needed.

Information may be stored electronically in a transponder or RFID "tag" and that
20 information is communicated to a tag "reader." Communication between the RFID tag
and reader is by the transmission and reception of electromagnetic (EM) waves, and each
must have an antenna to convert electrical signals to EM waves and vice versa. Low

power RFID systems can operate over a wide range of frequencies, including the high-frequency (HF) through super-high-frequency (SHF) radio bands, roughly 3 Megahertz (MHz) to 6 Gigahertz (GHz). RFID systems may also operate at much higher frequencies, including operation at or in the vicinity of 400 MHz, 915 MHz, 2.45 GHz in the ultra-high frequency (UHF) band and 5.88 GHz in the SHF band. The performance of an RFID tag operating in the high frequency (HF) band, for example at 13.5 MHz, is generally not affected by the tag's proximity to the human body. This is desirable for RFID tags used in identification bands. Coupling between the tag antenna and the reader antenna is primarily by the magnetic component of the reactive near field, in which the tag antenna is configured as a coil in a resonant circuit.

Because identification appliances may communicate with other devices, additional features and circuits may be desirable as well.

SUMMARY OF THE INVENTION

An identification appliance, such as a wristband, bracelet, patch, headband, neckband, ankleband, armband, belt, card, sticker, or other wearable appliance, is enhanced with a biometric sensor, chemical sensor, optical sensor, heat sensor, pressure sensor, humidity sensor, electromagnetic sensor, acoustic sensor, various opto-electronics and/or various security features such as tamper-evident and tamper-resistant features, as described herein. Also described are readers and verifiers for reading data from identification appliances, as well as applications for the identification appliance in passenger ticketing, passenger baggage accountability, passenger baggage claiming, and immigration status.

Other systems, methods, features and advantages of the invention will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the accompanying claims.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0001] The components in the figures are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention. Moreover, in the figures, like reference numerals designate corresponding parts throughout the different views.
- 10 However, like parts do not always have like reference numerals. Moreover, all illustrations are intended to convey concepts, where relative sizes, shapes and other detailed attributes may be illustrated schematically rather than literally or precisely.
- [0001] FIG. 1 illustrates an example of a prior art RFID wristband or bracelet.
- [0002] FIG. 2 is a representative illustration of an example embodiment of an improved
- 15 secure identification band.
- [0003] FIG. 3 is a representative illustration of another example embodiment of an improved secure identification band.
- [0004] FIG. 4 is a representative illustration of yet another example embodiment of an improved secure identification band.
- 20 [0005] FIG. 5 is a representative illustration of yet another example embodiment of an improved secure identification band, which contains ink that is released by tampering.
- [0006] FIG. 6 is a representative illustration of still another example embodiment of an

improved secure identification band, which, when attached, creates an identifying pattern in both visible and electronic forms.

[0007] FIG. 7 is a representative illustration of an example embodiment of an improved identification band that stores biometric information.

5 [0008] FIG. 8 is a representative illustration of another example embodiment of an improved identification band, which stores biometric and alphanumeric information.

[0009] FIG. 9 is a representative illustration of an example embodiment of an improved identification band, which stores biometric and alphanumeric information and whose circuit functions are activated when the band is attached or deactivated when the band is
10 unfastened, torn, cut, or overly stretched.

[0010] FIG. 10 is a representative illustration of an example method of using an improved identification band for passenger ticketing and boarding.

[0011] FIG. 11 is a representative illustration of an example method of using an improved identification band for passenger baggage tagging and claiming.

15 [0012] FIG. 12 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, which has printed biometric data.

[0013] FIG. 13 is a representative illustration of another example embodiment of an improved identification appliance, such as an identification band, with printed biometric data.

20 [0014] FIG. 14 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with a biometric sensor.

[0015] FIG. 15 is a representative illustration of another example embodiment of an

improved identification appliance, such as an identification band, which has a biometric sensor and a wireless communication circuit.

[0016] FIG. 16 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, which has a biometric sensor, a
5 wireless communication circuit such as a RFID circuit, and an electronic memory or data storage device.

[0017] FIG. 17 is a representative illustration of yet another example embodiment of an improved identification appliance, such as an identification band, with a biometric sensor and display.

10 [0018] FIG. 18 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with photovoltaic cells.

[0019] FIG. 19 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with embedded circuitry and a microstrip or patch antenna.

15 [0020] FIG. 20 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, which performs signal processing and computation and has an electronic data storage device or memory.

[0021] FIG. 21 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with one or more chemical
20 sensors.

[0022] FIG. 22 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with an acoustic sensor.

[0023] FIG. 23 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with electro-optical components.

[0024] FIG. 24 is a representative illustration of yet another example embodiment of an improved identification appliance, such as an identification band, with an optical sensor.

5 [0025] FIG. 25 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with a flexible keypad.

[0026] FIGs. 26A and 26B are representative illustrations of an example method of embedding silicon and/or printed circuitry, or other components, in an identification appliance such as an identification band.

10 [0027] FIGs. 27A and 27B are representative illustrations of an example method of implementing printed circuitry in an identification appliance such as an identification band.

[0028] FIG. 28 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with a flexible battery or power
15 source.

[0029] FIG. 29 is a representative illustration of another example embodiment of an improved identification appliance, such as an identification band, with a "button" style battery.

[0030] FIG. 30 is a representative illustration of an example embodiment of an improved
20 identification appliance, such as an identification band, which is partially disposable.

[0031] FIG. 31 is a representative illustration of another example embodiment of an improved identification appliance, such as an identification band, which is partially

disposable.

[0032] FIG. 32 is a representative illustration of an example embodiment of an improved identification appliance which is reusable.

5 [0033] FIGs. 33A, 33B and 33C are representative illustrations of example embodiments of a biometric reader/verifier of identification appliances.

[0034] FIGs. 34A, 34B and 34C are representative illustrations of example applications of a biometric identification appliance reader/verifier.

10 [0035] FIG. 35 is a representative illustration of an example embodiment of an improved secure identification appliance, such as an identification band, with electronic tamper detection.

[0036] FIG. 36 is a representative illustration of an example embodiment of an improved secure identification appliance, such as an identification band, with electronic tamper detection using conductive or non-conductive glue.

15 [0037] FIG. 37 is a representative illustration of an example embodiment of an airport security system which uses an improved secure identification appliance, such as an identification band.

[0038] FIG. 38 is a representative illustration of another example embodiment of an airport security system which uses an improved secure identification appliance, such as an identification band.

20

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As used in this specification, the meaning of "in," whether alone or in a compound such as "therein," includes "in" and "on"; "radio frequency identification" and

"RFID" refer to identification by radio frequency communication.

FIG. 1 illustrates an example of a prior art RFID wristband or bracelet 1. The substrate 2 is an elongated flexible strip of polymer or paper. The RFID circuit 3 comprises antenna circuitry, signal generator circuitry, programmable encoder circuitry and interconnection circuitry. A fastener to adjustably and securely attach the wristband 1 comprises, on one end of the substrate 2, a snap fastener with parts 4 and 8 which can close over the other end of substrate 2, through one of the adjusting holes 6 therein, and snap together. The circuitry comprising the RFID circuit 3 can be, in various combinations, carried in the substrate 2, or formed by deposition on a layer in the substrate 2 of one or more of conductive paths, semiconductor devices, or polymer materials, in accordance with U.S. Patent No. 5,973,598. The fastener can also comprise an adhesive wristband closure in accordance with U.S. Patent No. 5,457,906, a closure mechanism in accordance with U.S. Patent No. 5,479,797, a rivet, a staple, a crimp, or heat, which when applied, securely attaches the ends of the wristband to each other, which closes the wristband around the wearer's wrist.

FIG. 2 illustrates an example embodiment of an improved secure identification band 90. As with any of the embodiments described in this disclosure, an identification "band" may comprise a wristband, bracelet, patch, headband, necklace, card, sticker, or other wearable appliance. The identification band may include data that is perceivable to humans, animals, or machines. For example, the emission of an aerosol chemical or scent may be easily detectable by an animal such as a dog. Further, the data may be alphanumeric data, optical character recognizable data (such as bar codes), images,

photographs, magnetically readable data, and/or biometric data. Biometric data refers to data which can be used to identify a person such as the person's fingerprint, retina, blood, DNA, or voice data. In this particular example illustration, the identification band 90 includes a structure 91 that is suitable to be worn by, attached to, or carried by a person.

5 Preferably, the identification band 90 is a wristband and the structure 91 is an elongate, flexible wristband material. For example, the structure 91 may be an elongated flexible strip of polymeric, paper, or organic substrate. However, the identification band 90 need not be attached only to the wrist of a person as it also can be attached to the ankle, neck, or other part of a person or animal, or to an object. The fastening of the band 90 closes a

10 circuit 92 and enables circuit functions such as RFID functions. The improved band 90 comprises a substrate structure 91, a circuit 92, an electrically conductive fastener with parts 93 and 94, adjusting holes 95, and conductors 96 and 97 which connect the circuit 92 to each fastener part 93 and 94. As with any embodiment described in this disclosure, the circuit 92 preferably includes other circuits, such as antenna circuitry, communication

15 circuitry, signal generator circuitry, programmable encoder circuitry and interconnection circuitry. Further and as with any embodiments in this disclosure, the circuit may perform a variety of functions including communication functions such as RFID. In one embodiment, a surface mount RFID chip containing electronic circuits is mounted within the identification band and electrically connected to an antenna. The circuitry comprising

20 the communication circuit can be, in various combinations, carried in the substrate 91, or formed by deposition on a layer^{see note} in the substrate 91 of one or more of conductive paths, semiconductor devices, or polymer materials. A circuit consisting entirely of conductive,

2 Memory circuit

insulating and/or semiconductive materials directly deposited on the substrate 91 may also be used. In fact, any of the circuits on the identification band can be made either partially or totally from semiconductors, conductors and insulators, and may be fabricated of inorganic or organic materials, as described in U.S. Patent No. 5,973,598, the entire disclosure of which is incorporated herein by reference for all purposes. An exemplary technique for forming an organic device, such as an organic semiconductor, is described in an article by Garnier et al. entitled "All-Polymer Field-Effect Transistor Realized by Printing Techniques" (Science, Vol. 265, 16 September 1994), the entire article of which is incorporated herein by reference for all purposes. In other words, the identification band may have electronic components made either partially or totally from semiconductors, conductors and insulators, which may be inorganic or organic, and which may be printed on the identification band. U.S. Patent No. 5,973,598 describes organic components, any of which may be used in the improved identification band. Further, a memory containing organic material is described in U.S. Patent Application No. 2001000817107, titled "Integrated Circuit Provided with a Substrate and with a Memory, Transponder, and Method of Programming a Memory," issued November 29, 2001 to U.S. Philips Corp., the entirety of which is incorporated herein by reference for all purposes. It is preferable for the components of the identification band 90 to be thin so it is comfortable to wear. Additionally, it is preferable for the substrate 91 and the printed components to be flexible.

Further, as with any embodiment having a circuit, the circuit 92 of FIG. 2 may include a control logic or processing unit, which may be a microprocessor,

microcontroller, central processing unit (CPU), arithmetic logic unit (ALU), math coprocessor, floating point coprocessor, graphics coprocessor, hardware controller, programmable logic device programmed for use as a controller, or other control logic.

The circuit may include any of the circuits described in this disclosure or known to those of skill in the art of circuit design. The circuit further may include an optional data storage device, such as a memory of any kind. The data storage device or memory may be fabricated out of inorganic materials, organic materials, or a combination of inorganic and organic materials. The identification band 90, and any of the identification bands described in this disclosure, may include an antenna such as a microstrip antenna described in co-pending U.S. Patent Application Serial No. _____, titled Microstrip Antenna for an Identification Appliance, filed on March 5, 2002, whose entire disclosure is incorporated herein by reference for all purposes.

When the fastener closes, the parts 93 and 94 of the fastener come into contact, which closes the circuit 92 through the conductors 96 and 97, thereby enabling circuit functions. The conductors 96 and 97 may comprise two or more separate electrical conductors which are connected to the circuit 92; the conductors further may comprise one or more of conductive wire or fiber, conductive foil, meltable conductor, or a printed conductor. In communication with the conductors is a fastener comprising one or more of a conductive adhesive, a conductive closure mechanism, a magnetic closure mechanism, a conductive rivet or staple, a crimp or heat in proximity to the conductors, any of which when applied electrically connects or alters the capacitance between the conductors, thereby closing one or more electrical circuits which may, for example,

power the circuit 92, connect an antenna, tune the antenna, or change a logic state input to the circuit 92.

Other methods of fastening the identification band of any of the embodiments described in this disclosure include applying to the overlapping portions of the substrate one or more of the steps of permanently deforming the substrate to stitch together the overlapped portions, rupturing walls of adhesive-filled microspaces in the substrate and curing the adhesive by radio frequency, heat or ultraviolet exposure, rupturing walls of microspaces in the substrate separately filled with adhesive and catalyst which mix and cure thereupon, or by melting together adjacent surface areas of the overlapped portions, which when performed, securely attaches the ends of the wristband to each other, thereby closing the wristband around the wearer's wrist.

Yet another alternative is to attach the identification band by a means similar to a belt buckle. For example, the buckle may be mounted to one end of the substrate 91 and which when opened, allows free movement of the other end of the substrate through the buckle so that the band be adjustably fitted to the wearer. The buckle design also permits removal of the identification band from the wearer for reuse. The buckle may comprise an electrical conductor and circuit-activating means to activate the circuit 92 when the identification band is fastened and to deactivate the circuit 92 when the identification band is unfastened or removed. The buckle can be made of an electrically conductive metal of a type which is known to be suitable for buckles, including but not limited to an alloy of iron, copper or aluminum; the buckle can also be made of a polymer having an electrically conductive coating thereon. The circuit-activating means may comprise two

separate electrical conductors in the substrate 91, each of which separately connects to the circuit 92 and extends toward the end of the substrate which does not have the buckle. When the buckle closes and clamps the substrate 91 between the movable and fixed portions of the buckle, a direct contact or a capacitive gap forms between each conductor and the buckle conductor, thereby closing an electrical circuit which in turn activates the circuit 92. When the buckle is opened and the identification band is removed, the direct contact or capacitive gap between each conductor and the buckle conductor is broken, thereby opening the electrical circuit which in turn deactivates the circuit 92.

The securement of the identification band may be permanent for the usage life of the band, or may be temporary and defeatable by an authorized procedure. In the case of temporary securement, the identification band may be re-used and re-secured by an authorized agency or person.

Any of the identification appliances or bands described in this disclosure may have electromagnetic energy absorption means so that the identification band may be energized by an external electromagnetic field signal. For example, an antenna may obtain power from a received signal, where the power is used to power some or all of the circuits on the identification appliance. The interrogating/powering electromagnetic signal provides power and enabling information to the identification band. The interrogating/powering signals may contain a power signal only or both a power signal and information modulated onto the power signal. Upon energizing by an electromagnetic signal, the identification band may display optically readable information

according to the data programmed in the band, stored in the band, or received from the interrogating/enabling device.

Likewise, any of the identification appliance described in this disclosure may include an optional audio, visual, or sensory (e.g., vibrating) device to display
5 information such as the scanned biometric data and alphanumeric information. The display may be a light emitting polymer diode, a liquid crystal display (LCD), or a diode-capacitor directly connected to an antenna that may be a resonant antenna. An example of a diode-capacitor is provided in U.S. Patent Application Serial No. 09/723,897, titled
10 "Rectifying Charge Storage Element" and filed on November 28, 2000, the entirety of which application is incorporated herein by reference for all purposes. The display can be always on, turned on by the circuit in the identification band, or activated by an external electromagnetic field signal. If an interrogating/powering electromagnetic signal includes a power signal and data modulated onto the power signal, the display may indicate only the presence of an interrogating or powering field, or it may indicate the
15 data transmitted with the interrogating or powering field. Still alternatively, the display may indicate data derived from internal data in the identification band, a combination of information from both the identification band and the interrogating/powering field, or information derived from information from a combination of information from both the band and the field.

20 The display may consist of a single device or a plurality of devices. A single device may be formed in an arbitrary shape, including an alphanumeric character, logo, or other recognizable symbol or picture. A plurality of devices may be formed into a

matrix (row/column addressable) or another combination that creates a variety of different recognizable visual outputs such as pre-formed characters or symbols. The display may be based on an array of pixels. The display may be a flexible display formed on or attached to the substrate of the identification band. The display may be formed of
5 reflective technologies such as electrophoretic, ferroelectric, cholesteric, or emissive technologies such as organic LED (OLED), PDLC plasma (a reflective mode polymer-dispersed-liquid-crystal display), or cholesteric nematic (passive matrix LCD) technologies. A reflective display may be attached to or formed on the identification band, and the reflective display may be either volatile, where the display only produces
10 an optical output when electricity is powering it, or nonvolatile, where the display retains its optical state even after power is withdrawn from it. A nonvolatile display may be write-once or be re-programmable. The display may provide information that is optically readable as image data by humans or machines, or a time-varying modulated optical signal (e.g., from a light-emitting diode or composite organic light-emitting device) that
15 may be decoded remotely by an electro-optical receiver.

Any of the identification appliances or bands described in this disclosure may include an optional optical information transmission means so that information programmed or stored in the identification band may be transmitted optically as a modulated signal, through any of the known modulation techniques. Such an optical
20 device includes silicon and polymer light emitting diodes (LEDs).

FIG. 3 illustrates another example embodiment of an improved secure identification band 90. The band 90 has a circuit 92 which opens and disables certain

functions, such as communication or RFID functions, when the band is torn, cut, or overly stretched. The band 200 comprises a substrate 91, a circuit 92, a fastener with parts 93 and 94, adjusting holes 95, and a conductor 96 which forms a closed circuit with the circuit 92. When the band 90 is torn, cut, or overly stretched, the conductor 96
5 breaks, thereby opening the circuit and disabling circuit functions. The conductor 96 may comprise a pattern of electrical interconnections in the substrate 91, the conductors of which comprise one or more of a conductive wire or fiber, conductive foil, organic conductor, or printed conductor. When the band 90 is torn, cut, or overly stretched, the conductor 96 is severed or broken, thereby disconnecting portions of the circuit 92 which
10 may in turn power the circuit 92 off, disconnect an antenna, detune the antenna, or change one or more logic state inputs to the circuit 92.

Alternatively, circuit functions can also be disabled by using a pattern of non-conductive fibers in the substrate 91 which are stronger than substrate and electrical interconnections therein; when the band 90 is stretched or twisted, the fibers tear the
15 substrate 91 and rupture electrical circuits therein, which destroys or renders inoperative, for example, a data storage device in the circuit 92, a data transmission device in the circuit 92, some other circuit in the circuit 92, or the entire circuit 92. This alternative approach may be implemented in any of the other embodiments described in this disclosure.

20 FIG. 4 illustrates yet another example embodiment of an improved secure identification band 90. Band 90 has a circuit 92 which closes and enables certain circuit functions when the band 90 is fastened and which opens and disables certain circuit

functions when the band 90 is unfastened or is torn, cut, or overly stretched. As shown in FIG. 3, the band 90 comprises a substrate 91, a circuit 92, an electrically conductive fastener with parts 93 and 94, adjusting holes 95, and conductors 96 and 97 which connect the circuit 92 to each fastener part 93 and 94. When the fastener closes, the parts 5 93 and 94 of the fastener come into contact, thereby closing the circuit 92 through the conductors 96 and 97 and enabling circuit functions. When the band 90 is unfastened, or is torn, cut, or overly stretched and conductor 96 or 97 breaks, the circuit opens and disables certain or all circuit functions. The conductors 96 and 97 may comprise two or more separate electrical conductors which are connected to the circuit 92, the conductors 10 comprising one or more of conductive wire or fiber, conductive foil, meltable conductor, or a printed conductor. In communication with the conductors may be a fastener comprising one or more of a conductive adhesive, a conductive closure mechanism, a magnetic closure mechanism, a conductive rivet or staple, a crimp or heat in proximity to the conductors, any of which when applied electrically connects the conductors or alters 15 the capacitance between the conductors, thereby closing one or more electrical circuits which may, for example, power the circuit 92, connect an antenna, tune the antenna, or change a logic state input to the circuit 92. When the electrical circuits are opened by unfastening, stretching, or cutting the band 90, portions of the circuit 92 are disconnected which may power off portions or all of the circuit 92, disconnect an antenna, detune the 20 antenna, or change a logic state input to the circuit 92. As previously mentioned, circuit functions can be disabled alternatively by using a pattern of non-conductive fibers in the substrate 91 which are stronger than substrate 91 and electrical interconnections therein.

When the band 90 is overly stretched or twisted, the fibers tear or deform the substrate 91 and rupture electrical circuits therein, thereby destroying a data storage device in the circuit 92, a data transmission device in the circuit 92, any other circuit in the circuit 92, or the entire circuit 92.

5 FIG. 5 illustrates another example embodiment of an improved secure identification band containing an ink or dye which is released by tampering. As shown in FIG. 4, the example band 90 comprises a substrate 91, a circuit 92, a fastener with parts 93 and 94, adjusting holes 95, and container 98 containing an ink or dye 99 which is released when the band 90 is torn, cut, or overly stretched. The ink-releasing means
10 comprises an ink-filled space 98 in the band 90 and an empty space in the band 90 which is adjacent to the ink-filled space 98. When the band 90 is overly stretched, twisted, torn or cut, the wall ruptures between the ink-filled space 98 and the adjacent empty space, thereby leaking ink into the empty space and visibly discoloring the band 90.
Alternatively, the wall ruptures between the ink-filled space 98 and the exterior surface of
15 the band 90. In addition, the ink or dye may contain a chemical aerosol or scent perceivable by an animal, such as a dog.

 Alternatively, the identification band may be attached by means similar to a belt buckle, as previously discussed. For example, the buckle may be mounted to one end of the substrate 91 and which when opened, allows free movement of the other end of the
20 substrate through the buckle so that the band be adjustably fitted to the wearer. The buckle design also permits removal of the identification band from the wearer for reuse.
A dye tack in communication with the buckle releases dye when the buckle or dye-tack is

subjected to tampering. The dye or ink tack may be similar to those used for retail theft deterrence, has locking parts which can be removed intact only with a special tool, and is attached in such a manner that a portion of the dye tack closes over or around a portion of the closed buckle. When an unauthorized attempt is made to open the buckle or to
5 remove the dye tack from the identification band, a dye-filled vial in the dye tack is broken, thereby leaking dye out and discoloring identification band or marking the skin of the person who is tampering with the buckle or dye tack. Again, an aerosol chemical or scent may be contained in the dye tack, which is perceivable to an animal, human, or machine.

10 FIG. 6 illustrates still another example embodiment of an improved identification band 700 that, when attached, creates an identifying pattern in both visible and electronic forms. As shown in FIG. 6, the example improved identification band 700 comprises a substrate 705 having a circuit 710 and an identification area 715 with a shaded background into which conductor pairs 720 from the circuit 710 terminate with
15 connections 725. To attach the identification band 700, the first end 730 is placed over the second end 735, and holes 740 are punched through, or embossed into, area 715 with the aid of alignment marks 735, thereby stitching together the overlapped ends, forming a visible pattern, and connecting and/or disconnecting specific pairs of conductors 720 to form an electrical circuit of connected and/or disconnected pairs, which in turn set logic
20 state inputs to the circuit 710 corresponding to the pattern. As with any of the embodiments, encoding the identity of a person, object or entity includes forming a unique pattern of one or more of an arrangement of figures, symbols or characters, a bar

code, or a drawing corresponding to that identity. Forming a visible identification of the person, object or entity includes one or more of the steps of forming an embossment, activating colorless material in the substrate which becomes colored, or colorless adhesive and catalyst in the substrate becoming colored when mixed or cured, said
5 material or adhesive and catalyst being sensitive to applied pressure or heat, thereby making the pattern visible. Applying the identifying pattern to the mechanical securement device includes one or more of mechanically, electrically, or thermally engraving, cutting, impressing, or embossing the pattern. In an example of the use of such a band 700, a number corresponding to a security clearance level of the wearer, such
10 as the number "3", or an official seal can be applied at the time of attachment. Thus, a visible indication of that clearance, and an electronic indication based on the formed electrical circuit and transmitted by the circuit 710, are available for controlling access to a secure area or to classified information.

The data stored in the identification band may include any kind of information.
15 For instance, the data may comprise identity data, financial transaction data, or medical data. Any of the data may be encrypted prior to the data being stored in the identification band. As another example, bands with the same pattern and related information can be attached to a person and to a set of baggage, the pattern identifying both the person and an airline flight, so that only persons and baggage identified for that flight will be allowed
20 on the aircraft, and the person can only claim baggage having bands with that same pattern.

An alternative to any of the embodiments described in this disclosure is to

associate more than one identity with an identification band. For example, a first identifying pattern and a second identifying pattern may be stored or contained on the identification band. The first and second identifying patterns may manifest in different ways. As an example, the first identifying pattern forms a visible first identification, while the second identifying pattern forms electrical data in a data storage device in the identification band. Moreover, the first and second identifying patterns may be used to identify the same or different people. For instance, the first identifying pattern may be associated with the person who is distributing the identification band and the second identifying pattern may be associated with the wearer of the identification band.

10 A battery or power source, when generative, may be provided to power a memory, logic, circuit, or other function of the identification band essential to its useful operation. In order to safeguard the security of information stored in the identification band in any of the embodiments described, the identification band may have a battery which runs out of power at or within a predetermined time period or on a certain calendar
15 date/time, or a circuit which stops its operation or erases the stored information at or within a predetermined time period or on a certain calendar date/time. To make the battery life run out, the circuit may impose a fixed load on the battery, a programmable constant load on the battery, or upon the expiration of a timer, impose a load on the battery. Alternatively, the identification band may have a lock mode for data stored in a
20 data storage device such as a memory such that the data is not accessible without the proper equipment, password, and/or matching of identifying data with the user trying to gain access to the information.

OK!

5 electrical contacts 1035 for receiving biometric information to be stored in the data storage device 1030. For example and as with any embodiment described in this disclosure which may have a data storage device, the data storage device 1030 may be a random access memory (RAM), read only memory (ROM), programmable read only memory (PROM), electrically erasable PROM (EEPROM), organic PROM, organic

10 RAM, anti-fuse PROM, ultraviolet light erasable PROM (UVPROM), fixed disk media, flexible disk media, flash memory, tape, or any other storage retrieval means, or any combination of these volatile and non-volatile memory means. The data storage device or memory can include any of the data storage devices or memories described in this disclosure or known to those of skill in the art of such devices. Also, as with any

15 embodiment described in this disclosure, the data storage device or memory may further permit reading only, reading and writing, or writing only.

As an example of the use of the improved band shown in FIG. 7, at the time of attachment of the band 1000 to a wearer 1040, the wearer 1040 is scanned by a charge-coupled device camera 1045 communicating with an encoder 1050 which converts the

20 image signal to encoded image data and transmits that data through a cable 1055, a removable plug 1060 inserted into jack 1035, and into the data storage device 1030. After attachment of the band 1000 and storage of the image data therein, the plug 1060 is

detached from the jack 1035 and the wearer 1040 is free to move around. To later ascertain or verify the identity of the wearer 1040, the image data is transmitted by the circuit 1010 to a reader 1065, such as a RFID reader, decoded and rendered into a viewable image 1070, and then compared with the actual appearance of the wearer 1040.

- 5 Alternatively, the data may be programmed into the data storage device 1030 by electromagnetic coupling, such as through RF waves.

Optionally, certain biological characteristics of the wearer 1040 may be stored in the band 1000 by transferring encoded biometric data to the data storage device 1030 on the band 1000 by electric current, electric or magnetic fields, or electromagnetic waves.

10 For example, such biometric data may include any images of or data about the wearer's fingerprints, retina, iris, DNA, genetic data such as a portion of the wearer's genome sequence or genes, or face, or a time domain or frequency domain response of the wearer's voice, or a biochemical assay of the wearer's scent, blood, or breath. In other applications, the biometric data may be related to a person's signature, signature plus

15 handwriting dynamics, iris, retina, face recognition, voiceprint, voiceprint and voice stress, fingerprint, other skin pattern, chemical signature (e.g., smell, blood, sweat), DNA signature, genetic data, or some electric, magnetic, acoustic, or other biometric characteristic. Alternatively, the biometric sensor may provide data about the wearer for purposes other than for identification. For instance, the biometric sensor may be

20 incorporated into the identification appliance to monitor or detect the wearer's pulse rate, heart electrical signals, blood pressure, insulin levels and the like, where such biometric data may be transmitted to other devices (such as monitoring computers at a hospital)

constantly, intermittantly, or upon alert conditions. The biometric sensor may be coupled to a data storage device, communication circuit, optical data display, or other components of the identification band. The biometric data may be encoded, converted into a data format according to a predetermined data template, and stored in a data storage device on the identification appliance. To verify the identity of the wearer of the identification appliance, any known method of comparing the stored biometric data and the wearer's biometric data may be used. For example, one method may be to determine the probability of a match. As an example of such a method, an XOR ("exclusive or") operation can be performed on the stored biometric data and the wearer's current biometric data to produce a third data set indicating those items in the first and second data sets which are not identical. A higher number of non-identical items will indicate a higher probability that the wearer is not the person whose encoded biometric data is stored in the identification band, and that number can also be compared to threshold numbers above which there are various predetermined levels of such probability (e.g. high, intermediate, or low). In accordance with corresponding biological features, data items can also be weighted in proportion to their effects on the overall certainty of identity verification. For instance, fingerprint data may be given higher weight than iris data. The results of the data comparison can also be displayed in a manner suitable for human judgment of probability.

FIG. 8 illustrates another example embodiment of an improved identification band 1200 in which biometric information and alphanumeric information are stored. As shown in FIG. 8, the improved band 1200 comprises a substrate 1205 having an RFID

circuit 1210, a fastener with parts 1215 and 1220, adjusting holes 1225, a data storage device 1230 which is preferably a nonvolatile memory, and a jack 1235 for receiving encoded information to be stored in the data storage device 1230. A first set of receptacles within jack 1235 communicates with a first area in the data storage device 1230 which is reserved for biometric information, and a second set of receptacles communicates with a second area in the data storage device 1230 which is reserved for alphanumeric information. The jack 1235 may be configured to accept only one plug, or more than one plug, at a time.

As an example of the use of the improved band 1200 shown in FIG. 8, at the time of attachment of the band 1200 to a wearer 1240, the wearer 1240 is scanned by a charge-coupled device camera 1245 communicating with an encoder 1250 which converts the image signal to encoded image data and transmits that data through a first cable 1255, a first removable plug 1260 having pins 1262 which insert into the first set of receptacles within jack 1235, and into the area of the data storage device 1230 reserved for biometric information. Subsequently, the wearer 1240 enters a personal identification number ("PIN") 1265 shown in FIG. 12 as "5612" into keypad-encoder 1270 which converts the PIN sequence 1265 to encoded alphanumeric data and transmits that data through a second cable 1275, a second removable plug 1280 having pins 1282 which insert into the second set of receptacles within jack 1235, and into the area of the data storage device 1230 reserved for alphanumeric information. After attachment of the band 1200 to the wearer 1240, storage of the image and PIN data therein, and removal of plugs 1260 and 1280 from the jack 1235, the wearer is free to move around. To later ascertain or verify

the identity of the wearer, the image and PIN data are transmitted by the circuit 1210 to a reader 1285 such as a RFID reader, decoded and rendered into a viewable image and alphanumeric data on video screen 1290. The person making the verification can then compare the viewed image with the actual appearance of the wearer, and, for additional security, compare the viewed PIN to a PIN communicated by the wearer. Alternatively to an electrical connection to a jack, an electromagnetically coupled circuit such as those used in a RFID tag may be used to transfer data. This method requires no physical contact with the circuitry of the identification band.

[0039] FIG. 9 is a representative illustration of an example embodiment of an improved identification band, which stores biometric and alphanumeric information and whose circuit functions are activated when the band is attached or deactivated when the band is unfastened, torn, cut, or overly stretched. As shown in FIG. 9, the improved band 1400 comprises a substrate 1405 having a circuit 1410, an electrically conductive fastener with parts 1415 and 1420, adjusting holes 1425, a data storage device 1430 which is preferably a nonvolatile memory in the circuit 1410, a jack 1435 for receiving encoded biometric and alphanumeric information to be stored in the data storage device 1430, and conductors 1445 and 1450 which connect the circuit 1410 to each fastener part 1415 and 1420. When the fastener closes, the parts 1415 and 1420 of the fastener come into contact, thereby closing the circuit through the conductors 1445 and 1450, enabling circuit functions, and making the stored data available for transmission by the circuit 1410. When the band 1400 is unfastened, or is torn, cut, or overly stretched and conductor 1445 or 1450 breaks, the circuit opens and disables any or all circuit functions.

144
Optionally, the opening of the circuit may cause the circuit to alter or destroy any data stored in memory 1430. If the band 1400 is reattached, again closing the circuit through the conductors 1445 and 1450 and enabling circuit functions, the originally-stored data, having been altered, is no longer available for transmission.

5 FIG. 10 is a representative illustration of an example method of using an improved identification band for passenger ticketing and boarding, such as at an airport, boat dock, train station, bus station and the like. As shown in FIG. 10, when a passenger 1510 checks in at a ticket counter, ticket information 1520 and an image of the passenger 1510 from a charge-coupled device camera 1530 and/or other identifying data are stored
10 in a data storage device which is preferably a nonvolatile memory on the band 1540. The band 1540 is then attached to the wrist 1550 of the passenger 1510. Preferably, the band 1540 is the type in which the stored data is altered or destroyed when the band detects any tampering or detachment of the band. The band 1540 serves as a passenger ticket and boarding pass, and when the passenger 1510 is about to board, the stored data in the
15 data storage device on the band 1540 on the wrist 1550 may be transmitted to a reader 1560, decoded and verified either automatically or by a human viewing data on a video screen 1570 so that the identity and proper ticketing of passenger 1510 can be verified.

 FIG. 11 is a representative illustration of an example method of using an improved identification band for passenger baggage tagging and claiming. At departure,
20 identification bands 1610 are prepared with stored encoded passenger image or other identifying data and ticket information, one of which is attached to the passenger's wrist 1620 as a baggage claim receipt and the rest of which are attached to the passenger's

baggage items 1630 as baggage tags. At the baggage claim in the destination terminal, the stored data in the identification bands 1610 on the wrist 1620 and on the baggage items 1630 are transmitted to a reader 1640, decoded and verified automatically or by a human viewing data on a video screen 1650, so that the baggage items 1630 can be properly claimed by matching the bands 1610 to each other.

FIG. 12 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, which has printed biometric data. The example identification appliance has an elongate band 10, a band fastener 12, and a mating band fastener 14 that mates with the band fastener 12. The identification appliance can have printed information 16 and a portrait 18 or fingerprint 20.

FIG. 13 is a representative illustration of another example embodiment of an improved identification appliance, such as an identification band, with printed biometric data. The example identification appliance has an elongate band, a band fastener 26, and a mating band fastener 28 that mates with the band fastener 26. The elongate band may comprise a top laminate 22 and a bottom laminate 24. Silicon and/or printed circuitry components 30 may be sandwiched between the laminates 22, 24. The identification appliance may have printed biometric information 32 on any of its surfaces.

FIG. 14 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with a biometric sensor. The example identification appliance has an elongate band 34, a band fastener 36, and a mating band fastener 38 that mates with the band fastener 36. As with any of the embodiments described in this disclosure, silicon and/or printed circuitry components 40

may be embedded, printed, or otherwise deposited in or on the elongate band 34. The identification appliance may include a biometric sensor 42. The biometric sensor 42 may scan or otherwise obtain a person's fingerprint, iris, retina, or other identifying biometric feature and provide the biometric information to the circuitry 40. An example of such a biometric sensor built from an optical device is as follows. The optical device may include a layered structure containing a light emitting device(s) and semi-transparent light sensing devices for measuring light reflection of an object placed above the layered device. By using these optical devices, the reflective signature of a fingerprint could be illuminated, measured and recorded. The optical device may be a single device that senses the presence or absence of light wavelengths, the intensity of light wavelengths, or a time-varying optical signal carrying information. Alternatively, the optical device may comprise a plurality of sensing devices including a linear or two-dimensional array of sensors. The optical device may include a non-visible (i.e. infra-red or ultra-violet) optical input, optical output, or power conversion element. As with any of the described embodiments, the biometric sensor may be an optical sensor, a heat sensor, a pressure sensor, a humidity sensor, a chemical sensor, an electromagnetic sensor, or an acoustic sensor; the biometric sensor may be a plurality of devices that may be formed into a matrix (row/column addressable) or other spatially distributed pattern of elements. The circuitry 40 preferably includes other circuits, such as antenna circuitry, signal generator circuitry, communication circuitry, programmable encoder circuitry and interconnection circuitry, and is adapted to control and interact with the biometric sensor 42. The circuitry for the biometric sensor 42 may be made of silicon, organic materials, or other

thin materials. Further, biometric information 44 may be printed on the band 34. The circuitry 40 may then compare the scanned biometric data with stored biometric data to determine their correlation. The identification appliance, as with any of the embodiments described in this disclosure, may include an audio, visual, or sensory (e.g., vibrating) device to indicate whether a correlation or match exists. As with any embodiment described in this disclosure, an optional antenna, electronic data storage device or memory, battery or power source, display, and/or printed biometric or alphanumeric information may be included as well.

FIG. 15 is a representative illustration of another example embodiment of an improved identification appliance, such as an identification band, which has a biometric sensor and a wireless communication circuit such as a RFID circuit. The example identification appliance has an elongate band 46, a band fastener 48, a mating band fastener 50 that mates with the band fastener 48, silicon and/or printed circuitry components 56 which may be embedded or printed or otherwise deposited in or on the elongate band 46, a communication antenna 52 such as a RFID antenna which may be embedded or attached to the band 46, a biometric sensor 54, and printed biometric information 58 printed on the band 46. The biometric sensor 54, as with any of the embodiments in this disclosure, may scan a person's fingerprint, iris, retina, voice, or other identifying biometric feature. Of course, there may be more than one biometric sensor if desired. The biometric sensor 54 may be disposed in the elongate band 46, a securement structure used to fasten the identification band to a person, or both.

FIG. 16 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, which has a biometric sensor, a wireless communication circuit such as a RFID circuit, and an electronic memory or data storage device. The example identification appliance has an elongate band 60, a band fastener 62, a mating band fastener 64 that mates with the band fastener 62, silicon and/or printed circuitry components 74 which may be embedded or printed or otherwise deposited in or on the elongate band 60, a communication antenna 68 such as a RFID antenna which may be embedded or attached to the band 60, a biometric sensor 70, an electronic memory 72, and printed biometric information 66 printed on the band 60. The circuitry 74 preferably includes other circuits, such as antenna circuitry, signal generator circuitry, communication circuitry, programmable encoder circuitry and interconnection circuitry, and is adapted to control and interact with the biometric sensor 70 and electronic memory or data storage device 72. As with any embodiment described in this disclosure, the data storage device 72 may be any kind of memory or data storage device.

The biometric sensor 70 may scan a person's fingerprint, iris, retina, voice, or other identifying biometric feature. Of course, there may be more than one biometric sensor if desired. The circuitry 74 may then compare the scanned biometric data with biometric data stored in the data storage device 72 to see if they match. The identification appliance may include an audio, visual, or sensory (e.g., vibrating) device to display the biometric data and/or to indicate whether a match exists, which device may optionally communicate the data remotely to a remote sensor or display device; such a display can

be any of the displays described in this disclosure or known to those of skill in the art of displays.

FIG. 17 is a representative illustration of yet another example embodiment of an improved identification appliance, such as an identification band, with a biometric sensor
5 82 and display 88. The identification appliance of FIG. 17 is similar to that of FIG. 16, except that FIG. 17 specifically illustrates a display 88. The example identification appliance has an elongate band 76, a band fastener 78, a mating band fastener 80 that mates with the band fastener 78, silicon and/or printed circuitry components 84 which may be embedded or printed or otherwise deposited in or on the elongate band 76, a
10 communication antenna 86 such as a RFID antenna which may be embedded or attached to the band 76, and a biometric sensor 82. The biometric sensor 82 may sense or scan a person's fingerprint, iris, retina, voice, or other identifying biometric feature. The circuitry 84 may then compare the scanned biometric data with biometric data stored in the data storage device to determine if they match. The display 88 may display the
15 biometric data and/or to indicate whether a match exists in a manner perceptible to a person, such as by an audible, visual, or sensory (e.g., vibrating) device. An optional antenna, electronic data storage device or memory, acoustic sensor, chemical sensor, optical sensor, heat sensor, pressure sensor, humidity sensor, electromagnetic sensor, flexible keypad, battery or power source, and/or printed biometric or alphanumeric
20 information may be included as well. As with any of the embodiments described in this disclosure, these optional devices and sensors may be disposed in the elongate band, a securement structure used to fasten the identification band to a person, or both.

FIG. 18 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with photovoltaic cells. The example identification appliance has an elongate band 100, a band fastener 102, a mating band fastener 104 that mates with the band fastener 102, silicon and/or printed circuitry components 106 which may be embedded or printed or otherwise deposited in or on the elongate band 100, and photovoltaic cells 108. The photovoltaic cells 108 provide power, and optionally information such as power status, to the circuitry 106. To generate photoelectric power, a photodiode (formed of silicon, amorphous silicon, or organic material) or photodiode array may be attached to or formed on the identification band.

The photodiode could generate electric power to power the circuitry on the band, or recharge a battery attached to or formed on the band. The photodiode can also serve as a signal input transducer for information input to the identification band, which information may be transmitted to the identification band by a light source modulated by the information content. As with any embodiment described in this disclosure, an optional antenna, electronic data storage device or memory, biometric sensor, acoustic sensor, chemical sensor, optical sensor, heat sensor, pressure sensor, humidity sensor, electromagnetic sensor, flexible keypad, battery or power source, display, and/or printed biometric or alphanumeric information may be included as well.

FIG. 19 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with embedded circuitry and a microstrip or patch antenna. The example identification appliance has an elongate band 110, a band fastener 112, a mating band fastener 114 that mates with the band fastener

112, silicon and/or printed circuitry components 118 which may be embedded or printed or otherwise deposited in or on the elongate band 110, printed biometric information 116, and a microstrip or patch antenna 120. The microstrip antenna 120 may be any of those described in co-pending patent application filed concurrently, titled "Microstrip Antenna
5 for Identification Appliance", U.S. Patent Application Serial No. 09/_____, the entirety of which application is hereby incorporated by reference for all purposes. Such a microstrip antenna provides certain advantages, such as directing more of the radiating energy away from the wearer to improve the transmission range of the identification appliance and to reduce directing energy toward the wearer for health reasons. The
10 microstrip antenna may be added or deleted from any of the embodiments described in this disclosure.

FIG. 20 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, which performs signal processing and computation and has an electronic data storage device or memory. The example
15 identification appliance has an elongate band 122, a band fastener 124, a mating band fastener 126 that mates with the band fastener 124, silicon and/or printed circuitry components 132 which may be embedded or printed or otherwise deposited in or on the elongate band 110, printed biometric information 128, an antenna 130 and an electronic data storage device or memory 134. The circuitry 132 may include signal transmission
20 circuitry, signal reception circuitry, data processing circuitry and computation circuitry, as desired. In this example, the circuitry 132, data storage device 134 and antenna 130

are sandwiched between the inner substrate of the body 122 and the structure carrying the printed information 128.

FIG. 21 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with one or more chemical
5 sensors 144. The example identification appliance has an elongate band 136, a band fastener 138, a mating band fastener 140 that mates with the band fastener 138, silicon and/or printed circuitry components 142 which may be embedded or printed or otherwise deposited in or on the elongate band 136, and an antenna 143. Further, an optional
10 antenna, electronic data storage device or memory, biometric sensor, acoustic sensor, optical sensor, heat sensor, pressure sensor, humidity sensor, electromagnetic sensor, flexible keypad, battery or power source, display, and/or printed biometric or alphanumeric information may be included. The chemical sensor may be any kind of chemical sensor. For example, it may sense physiological attributes of a person such as temperature, sweat content and pheromones.

15 FIG. 22 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with an acoustic sensor 164. Of course, a plurality of acoustic sensors may be provided, if desired. The acoustic sensors may comprise audio transducers for audio input or output. An audio signal such as speech from the wearer may be transduced and processed by known techniques and
20 transmitted by the communication circuit in the identification appliance to a remote listener. Similarly, an audio signal may be received by the identification appliance from a remote transmitter by wireless communication, and processed and transduced to be

audible to the wearer. The identification appliance also may have known algorithms to process speech recognition or output synthesized speech. The acoustic sensor 164 may comprise a piezoelectric transducer that detects sound waves. Other types of acoustic sensors may also be used. The sound waves may be processed by a circuit 162, which
5 may include any known voice activation or speech recognition algorithms. Further, the appliance may allow users to communicate two-way with remote units or have circuitry or algorithms to derive biometric data (such as a user's unique identifying speech patterns) from the user's speech. The example identification appliance has an elongate band 154, a band fastener 156, a mating band fastener 158 that mates with the band
10 fastener 156, silicon and/or printed circuitry components 162 which may be embedded or printed or otherwise deposited in or on the elongate band 154, and printed biometric information 160. Further, an optional antenna, electronic data storage device or memory, biometric sensor, chemical sensor, optical sensor, flexible keypad, battery or power source, and/or display may be included as well.

15 FIG. 23 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with electro-optical or opto-electronic components 172. The example identification appliance has an elongate band 166, a band fastener 168, a mating band fastener 170 that mates with the band fastener 168, and silicon and/or printed circuitry components 174 which may be embedded or
20 printed or otherwise deposited in or on the elongate band 166. The circuit 174 may control the electro-optical components 172. For example, the electro-optical components 172 may perform various functions such as communicating optically with an external or

internal device, signaling (e.g., by light from a light emitting diode), indicating (e.g., by emitting light or varying light reflectances), displaying (e.g., of alphanumeric or image data by pre-formed indicators or matrix of indicators), sensing (e.g., of levels of light), and converting power (e.g., as a photovoltaic cell). As a further example, the electro-optical components 172 may comprise light emitting diodes (LEDs) which can be polymeric or organic LEDs as described in U.S. Patent No. 5,973,598. If the electro-optical components 172 perform an optical communication function, they may include optical fibers, light sources and/or light detectors such as photodetectors. If desired, the electro-optical components 172 may act as an electro-optical display device by including liquid crystal displays, electrophoretic displays, gas discharge displays and electromechanical displays. If desired, the electro-optical components 172 may include an electro-optical input device by including photodiodes, photoresistors, photomultiplier tubes and other input devices. The electro-optical components 172 may be of silicon or other materials, while some electro-optical components 172 may be fabricated partially or predominantly of organic compounds. They may be inflexible and attached on the identification appliance. Alternatively, they may be flexible and attached to or printed on the identification band. The electronic, electro-optical and visual components may be printed or otherwise deposited on the identification appliance's elongate structure (e.g., 91 in FIG. 2, 10 in FIG. 12).

FIG. 24 is a representative illustration of yet another example embodiment of an improved identification appliance, such as an identification band, with an optical sensor 198. The example identification appliance has an elongate band 188, a band fastener

190, a mating band fastener 192 that mates with the band fastener 190, printed information 194, and silicon and/or printed circuitry components 196 which may be embedded or printed or otherwise deposited in or on the elongate band 188. The circuit 196 may control the optical sensor 198. For example, the optical sensor 198 may
5 perform optical communication with an external or internal device. The optical sensor 198 may comprise a light detector such as a photodetector, or a charge coupled device to capture images of, for example, a person's face, fingerprint, iris, or retina.

FIG. 25 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with a flexible keypad 206. The
10 example identification appliance has an elongate band 200, a band fastener 202, a mating band fastener 204 that mates with the band fastener 202, silicon and/or printed circuitry components 208 which may be embedded or printed or otherwise deposited in or on the elongate band 200, and an antenna 210. The circuit 208 may control the keypad 206. Of course, the keypad 206 may comprise a full typewriter keyboard, a partial keyboard, a
15 single key, or a plurality of custom function keys. The keypad 206 permits users to input data into the circuit 208 or an optional data storage device. The keypad may be based on symbolic or alpha-numeric data.

FIGs. 26A and 26B are representative illustrations of an example method of embedding silicon and/or printed circuitry, or other components, in an identification
20 appliance such as an identification band. A top laminate 212 and a bottom laminate 214 may be adhered to each other. As shown by reference numeral 218, silicon and/or printed circuitry 216 and other components may be formed or printed on either the top or

bottom laminates 212, 214, or both laminates, and additional components may be sandwiched between the top and bottom laminates 212, 214. A manufacturing assembly is illustrated in FIG. 26B. The bottom laminate material 214 is fed at 220 and a machine 224 adheres circuitry 216 and other components to the bottom laminate 214. The top
5 laminate material 214 is fed at reference numeral 222 and joined to the bottom laminate 216 by laminating machine 226. A cutting device 228 separates the joined material into separate identification appliances. Of course, in any of the manufacturing processes described in this disclosure, other manufacturing steps known to those of skill in the art of making identification appliances may be used as desired.

10 FIGs. 27A and 27B are representative illustrations of an example method of implementing printed circuitry in an identification appliance such as an identification band. The body material is fed at 230 and a machine 232 prints or deposits circuitry and other components onto the body material. The machine may be an ink jet printing device, stencil, or any other method of imprinting inks or materials on a substrate. A
15 cutting device 234 separates the body material into separate identification appliances. In FIG. 27B, a bottom laminate material is fed at 238 and a machine 236 prints or otherwise deposits circuitry and other components onto the bottom laminate. The top laminate material is fed at reference numeral 240 and joined to the bottom laminate by laminating machine 242. A cutting device 244 separates the joined material into separate
20 identification appliances. Of course, other manufacturing processes known to those of skill in the art of making identification appliances may also be used as desired.

FIG. 28 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band, with a flexible battery or power source 258. In this particular example, the identification appliance has an elongate band formed out of a top laminate 246 and a bottom laminate 248. A band fastener 252 mates
5 with another band fastener 254. Silicon and/or printed circuitry components 260 also may be embedded or printed or otherwise deposited in or between the laminated band. The flexible battery 258 powers the circuit 260 as well as any other component on the identification appliance requiring power. Such other components may include, for example, an electronic data storage device or memory, biometric sensor, acoustic sensor,
10 chemical sensor, optical sensor, flexible keypad and display. Preferably, the battery 258 is thin and flexible. The battery 258 may provide primary or auxiliary power for electronic circuits. Optionally, the battery 258 may include a photovoltaic component so that the battery is charged or recharged by ambient light; the photovoltaic cells and recharging circuitry can be formed out of inorganic or organic materials. The battery 258
15 may be replaceable or not. The battery 258 may be a flexible polymer battery imprinted on or constructed on the identification appliance substrate, as described in U.S. Patent No. 5,973,598. The battery 258 may be activated when the identification appliance is fastened to its object, or activated by the reception of an optical signal or an electromagnetic signal. An identification appliance with a battery 258 may be activated
20 upon proper authorization or the start of service.

FIG. 29 is a representative illustration of another example embodiment of an improved identification appliance, such as an identification band, with a "button" style

battery 269. The example identification appliance has an elongate band 261, a band fastener 262, a mating band fastener 263 that mates with the band fastener 262, silicon and/or printed circuitry components 264 which may be embedded or printed or otherwise deposited in or on the elongate band 261, and printed information 265. The battery 269 is a button-style battery in this example embodiment. The battery 269 powers the circuit 264 as well as any other component on the identification appliance requiring power. Such other components may include, for example, an electronic data storage device or memory, biometric sensor, acoustic sensor, chemical sensor, optical sensor, flexible keypad and display. Preferably, the battery 269 is small and thin. The battery 269 may provide primary or auxiliary power for electronic circuits. The battery 269 is preferably replaceable.

Any of the identification appliance embodiments described in this disclosure may be completely disposable, partially disposable, or reusable. The disposable identification appliance may incorporate any of the functions described in this disclosure, where the fastening means is not re-usable and the functionality of the identification appliance is destroyed after its use. The identification appliance may have a disposable section (for example, the band) and a re-usable section (for example, the circuit). The identification appliance also may be made water resistant, waterproof, and/or resistant to certain solvents or chemicals used in the area of its application. If disposable, the band or body is preferably made of an inexpensive material such as paper, plastic, or other laminate material. For example, FIG. 30 is a representative illustration of an example embodiment of an improved identification appliance, such as an identification band,

which is partially disposable. The identification appliance comprises a disposable band 284 and a non-disposable "hub" 282 of circuitry, sensors and other circuit components. The band 284 is fastened by inserting one end 288 of the band to the non-disposable hub 282, which attachment is made more secure by a fastener 286, and by inserting the other
5 end 290 of the band to the non-disposable hub 282, which attachment is made more secure by a fastener 286. When desired, the disposable band 284 may be unfastened from the non-disposable hub 282 and disposed. A replacement band may be fastened to the non-disposable hub 282. If the replacement band is for a different user, any data stored in the non-disposable hub 282 may be erased and updated.

10 FIG. 31 is a representative illustration of yet another example embodiment of an improved identification appliance which is partially disposable. The identification appliance comprises a disposable flexible plastic or rubber tube 292, which acts as a band and houses an insertable and reusable circuit portion 294. The circuit portion 294 may include any kind of circuits such as communication circuitry and biometric circuitry.

15 FIG. 32 is a representative illustration of an example embodiment of an improved identification appliance which is reusable. This example identification appliance comprises a non-disposable band 298, which may be decorative to resemble jewelry or a watch. In or on the band 298 is disposed non-disposable circuitry, sensors and components 296. An optional lock mechanism 300 may be provided to secure the
20 identification appliance to a wearer and to allow the wearer to adjust its size. The lock mechanism may be activated or inactivated either by the wearer or alternatively by the person or agency responsible for providing the security function performed by the

identification appliance. The locking may be mechanical or electromechanical. The locking or un-locking function may be performed by remote communication or control, if desired.

FIGs. 33A, 33B and 33C are representative illustrations of example embodiments of a biometric reader/verifier of identification appliances. A biometric sensor 302 is mounted on a grip 306. The biometric sensor 302 may be any of the biometric sensors known to those of skill in the art of biometrics and those described in this disclosure. An interrogator 308 communicates, such as by radio frequency, to the identification appliance in order to obtain the biometric data stored in the appliance. An optional indicator or alarm system 304 may provide an audible, visible, or other perceptible indication as to, for example, whether the biometric data obtained by the biometric reader/verifier matches the biometric data stored in an identification appliance. Turning to FIG. 33B, the grip 306 may have a biometric sensor 302 and indicator 304 built into the handle of the grip. FIG. 33C is a representative illustration of a wearer of an identification appliance using an example embodiment of a reader/verifier. The user grasps the grip 306, thereby positioning the identification appliance 307 within range of the interrogator 308. The interrogator 308 communicates, such as by radio frequency, with the identification appliance 307 in order to obtain the biometric data and/or other data stored in the appliance.

FIGs. 34A, 34B and 34C are representative illustrations of example applications of a biometric identification appliance reader/verifier. In particular, FIG. 34A is a representative illustration of an example embodiment of a biometric turnstile system:

The turnstile system allows authorized personnel to pass between the turnstile arm 328 and a post 319. Device 318 may emit beams 322 which are used to detect whether anyone is at the turnstile arm, or trying to go under the turnstile arm 328. The device 318 may include a reader/verifier of identification appliances. When a person wearing an
5 identification appliance approaches the turnstile arm 328, the beams 322 detect the person and read identifying information, such as biometric data, from the identification appliance. If the identifying information gives the wearer the privilege or authority to pass, the turnstile arm 328 may be rotated out of the way to permit the wearer to pass. If, however, the wearer lacks the privilege to pass, an optional visible alarm system 320
10 and/or audible alarm system 332 may indicate that an unauthorized person is present.

FIG. 34B is a representative illustration of the details of an alternative biometric turnstile arm which may be used in FIG. 34A. The turnstile arm comprises a biometric sensor 312, a grip 314 with an optional built-in biometric sensor and an interrogator 316. The turnstile arm has an axis 330 of rotation. The biometric sensor 312 may be any of
15 the biometric sensors known to those of skill in the art of biometrics and those described in this disclosure. The interrogator 316 communicates, such as by radio frequency, to the identification appliance in order to obtain identifying biometric data stored in the appliance. An optional indicator or alarm system may provide an audible, visible, or other perceptible indication as to, for example, whether the biometric data obtained by
20 the biometric sensor 312 matches the stored biometric data obtained from the identification appliance.

FIG. 34C is a representative illustration of another example embodiment of an biometric gate. A turnstile 326 prevents people from entering a restricted area, such as a secure area or an amusement park. The turnstile includes a curved interrogator 324, which in the alternative, may have any suitable shape for reading a person's identification
5 appliance. In the example illustrated in FIG. 34C, a person wanting to gain access inserts his identification appliance, such as an identification wristband, into the vicinity of the interrogator 324. The interrogator 324 communicates, such as by radio frequency, to the identification appliance in order to obtain identifying biometric data stored in the appliance. The turnstile may include an optional biometric sensor 325 which obtains the
10 person's biometric data (e.g., fingerprint, iris, retina scan). The interrogator 324 compares the person's biometric data from the biometric sensor 325 and compares the data to the biometric data obtained from the identification appliance. An optional indicator or alarm system may provide an audible, visible, or other perceptible indication as to whether there is a match or non-match of biometric data.

15 FIG. 35 is a representative illustration of an example embodiment of an improved secure identification appliance, such as an identification band, with electronic tamper detection. The example identification appliance has an elongate body 342, a first patch of a plurality of conductive contacts 344, a second patch of a plurality of conductive contacts 346 and a securing device 347. When the securing device 347 is closed (to
20 fasten the identification appliance to a wearer), a physical and electrical contact is formed between contacts 344 and 346. The groups of contacts 344, 346 may be formed in patterns such that when the identification appliance is secured by device 347, the

resulting pattern of closed electrical contacts may be random or unpredictable. Circuitry 348 which may be embedded, printed, deposited, or otherwise placed in or on the band 342 monitors whether the electrical contact is open or closed. If a closed electrical contact is opened, the circuit 348 determines that the identification appliance has been
5 tampered with or removed. Optionally, the identification appliance may have an indicator to indicate the status of the identification appliance.

FIG. 36 is a representative illustration of an example embodiment of an improved secure identification appliance, such as an identification band, with electronic tamper detection using conductive or non-conductive glue. The example identification appliance
10 comprises an elongate body 358, a first patch of a plurality of conductive contacts 360, and a second patch of a plurality of conductive contacts 362 which mates with the first patch of contacts 360 to form a closed electrical circuit when the band 358 is closed. Circuitry 364 which may be embedded, printed, deposited, or otherwise placed in or on the band 358 monitors whether the electrical circuits are open or closed. An adhesive gel
15 366 may be used to close or fasten the ends of the band 358 together. The adhesive 366 may be conductive or nonconductive. As with the embodiment of FIG. 35, the groups of contacts may be closed in a random or unpredictable pattern.

FIG. 37 is a representative illustration of an example embodiment of an airport security system 500 which uses an improved secure identification appliance, such as an
20 identification band. A user or passenger 502 obtains an identification appliance 504, such as a wristband, from an authorized person or agency, such as the ticket counter. When the passenger 502 checks in baggage at the ticket counter or curbside check-in 506,

an identification band ("bag band") 508 is put on the baggage. The bag band 508 identifies the baggage and its owner so that when the passenger 502 goes to the baggage claim 510 to claim the baggage, corresponding data in the bag band 508 and passenger's identification appliance 504 must match. One way to determine whether there is a match is to use a band reader 512. The band reader 512 reads both the bag band 508 and passenger's identification appliance 504 and determines whether there is a match and optionally, whether there is any evidence of tampering of either. When the passenger 502 goes to the airline gate terminal 514, there may be another optional band reader to verify the identity of the passenger 502. Likewise, when the passenger 502 is about to board the aircraft 516, another optional band reader may verify the identity of the passenger 502 again. Throughout the airport, terminal, gates, restaurants, baggage areas and restrooms, there may be sensors 518 which detect and read any identification appliances 504 in their vicinity. A central airport system 520 may be coupled to the sensors 518 and band readers 512 so that the system 520 can track the whereabouts of each passenger.

FIG. 38 is a representative illustration of another example embodiment of an airport security system 500 which uses an improved secure identification appliance, such as an identification band. FIG. 38 illustrates an example checkin, departure and arrival process based on the airport security system 500. The left side of FIG. 38 depicts a passenger 502 and his baggage 505 at check-in and prior to departure. The middle section shows the check-in and departure process. Again, the passenger 502 obtains an identification appliance 504, such as a wristband, from an authorized person or agency, such as the ticket counter. When the passenger 502 checks in baggage 505 at the ticket

counter or curbside check-in, a bag band machine 507 creates a bag band 508 for the baggage 505 and an identification band 504 for the passenger 502. Alternatively, the bag band machine 507 may be a bag band reader. As before, the bag band 508 identifies the baggage and its owner. When the passenger 502 goes to the baggage claim 510 to claim
5 the baggage 505, the bag band 508 and passenger's identification appliance 504 must match. A band reader 512 may be used to read the bag band 508 and the identification band 504. Alternatively, if bag band machine 507 is adapted to read bag bands, the bag band reader reads the bag band 508 and another band reader reads the identification band 504. A baggage routing system 522 uses the bag bands to identify baggage and other
10 information necessary to route the baggage to its destination. Optional band readers 512 and sensors 518 may be placed at the gate 514, entry to or exit from the airplane 516, baggage claim 510 and any other area in the airport facility. The central airport system 520 may be coupled to the sensors 518 and band readers 512 so that the system 520 can track the whereabouts of each passenger as well as baggage. The central airport system
15 520 may be connected, if desired, to an international airport computer network 524 so that information is shared with other airports. The shared information may include an airport's information about passengers at the airport as well as international databases about known terrorists, fingerprints, etc. Thus, if airports detect that a group of known terrorists have entered into various airports at similar times, this fact can be made
20 available to the proper authorities such as the FBI. As another example, if an airport detects the presence of several known terrorists in the airport, the airport can enter a security mode, delay flights alert the appropriate authorities, and track the terrorists.

Upon arrival, the passenger 502 leaves the airplane and enters the gate 514. Again, a band reader 512 or sensor 518 may detect and ascertain the identity of the passenger 502 as he walks to the baggage claim 510. The identification band 504 and bag band 508 may be deactivated upon completion of the travel event.

5 Any of the identification appliance embodiments may be used also by immigration officials. There are situations in which the security of a remotely readable identification appliance and data carrier require that the identification appliance can only be secured to the person by an authorized person or agency, and once secured to the person being identified, cannot be removed or its data used except by an authorized party
10 or agency. Accordingly, the improved identification appliance can be supplied by U.S. Embassies or corresponding agencies throughout the world, which identification appliance can be encoded or encrypted with the identification and/or biometric features of the lawful bearer. The immigration authorities can read the identification appliances at the port of entry or authorized check points and compare the information retrieved from
15 the identification appliances to information stored in their database and to biometric information obtained at the present location.

 The identification appliance can be in the form of a single or multiple, detachable RFID/biometric labels which could then be detached and used to be affixed to paperwork, including a place in the Passport near the Visa seal, and which could be read and
20 removed upon departure in order to update and close open files on visitors to the U.S., such as temporary workers, students, business visas and tourists. With regard to the immigration Green Cards issued to lawfully admitted residents, the identification

appliance can be in the form of a temporary RFID/biometrics technology based label or card which identifies the bearer between the time of entry or admission to the U.S., and the mailing of the permanent card to the legal alien.

5 An additional use for the identification appliance would be to identify applicants for driver's licenses throughout the country. Driver's licenses are restricted to applicants who have proper and lawful identification that proves either proper citizenship or legal resident status. Exceptions are people with business visas on a temporary stay, some temporary working visas and perhaps people under student visas. An identification appliance with biometrics can be used to prove a person's identity and right to apply for a
10 driver's license.

In any of the embodiments, the identification appliance may include optional structures and features, such as any of the features described below. For example, the communication circuit may perform a communication function of any type and frequency, can communicate passively such as a transponder and/or actively by initiating
15 communications, and can use low or high frequencies. The identification appliance may operate in the low frequency, high frequency, UHF, SHF, or microwave radio bands.

The identification appliance may be attached to an article in which a circuit in the identification appliance performs an optional electronic article surveillance (EAS) function, for example, to prevent the theft of the article. The EAS function does not
20 transmit an identification code, but enables a reader to detect if the identification appliance is near the reader, for example, at the entry or exit to a retail store or building.

The identification appliance may provide its location to another device, for example, over a small area (e.g., a room or a building) or a large area (e.g., countrywide or worldwide). Such location information may be provided with a varying degree of accuracy such as with a less than 1 meter uncertainty to a greater than 1 kilometer
5 uncertainty. The location function may be accomplished by calculations derived by the identification appliance of signals received by it (such as from a Global Positioning System or a Local Positioning System), or the location may be derived externally to the identification band, such as by a matrix of RF receivers responding to the strength or timing of reception of signals received from the identification band.

10 In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. For example, the reader is to understand that the specific ordering and combination of process actions shown in the process flow diagrams described herein is
15 merely illustrative, and the invention can be performed using different or additional process actions, or a different combination or ordering of process actions. As another example, each feature of one embodiment can be mixed and matched with other features shown in other embodiments. Features and processes known to those of ordinary skill in the art of identification appliances may similarly be incorporated as desired. Additionally
20 and obviously, features may be added or subtracted as desired. Accordingly, the invention is not to be restricted except in light of the attached claims and their equivalents.

Patent
269/223

269/223
PATENT

CLAIMS

What is claimed is:

- IND X 1. **[[SECURE BAND: FIG. 2]]** An identification appliance adapted to provide information about a person, the identification appliance comprising:
- 5 a structure adapted to be worn by or attached to the person;
a fastener disposed in or on the structure, the fastener being adapted to attach the structure to the person; and
a circuit disposed in or on the structure and electrically coupled to the fastener, the closing of the fastener enables a function of the circuit.
- 10 ✓ 2. The identification appliance of claim 1 wherein the circuit function includes the communication of the information about the person external to the identification appliance.
- ✓ 3. The identification appliance of claim 1 wherein the circuit function includes the supply of power to the circuit.
- 15 ✓ 4. The identification appliance of claim 1 wherein the circuit function includes the enablement of an antenna.
- ✓ 5. The identification appliance of claim 1 wherein the circuit function includes the tuning of an antenna.
- ✓ 6. The identification appliance of claim 1 wherein the circuit function includes changing a logic state input to the circuit.
- 20 ✓ 7. The identification appliance of claim 1 wherein the structure is elongate and flexible.
- ✓ 8. The identification appliance of claim 1 wherein the circuit includes a radio frequency identification circuit, the radio frequency identification circuit adapted to transmit the information by radio frequency communication to an external device.
- 25 ✓ 9. The identification appliance of claim 1 wherein the fastener comprises a first contact and a second contact and the circuit determines whether the

first and second contacts are in electrical communication.

- 5
- ✕ 10. The identification appliance of claim 1 further comprising an electrical conductor which, when the fastener is closed, couples the fastener to the circuit, the conductor comprising one or more of a conductive wire or fiber, a conductive foil, a meltable conductor, or a conductor printed on the structure.
- 10
- ✕ 11. The identification appliance of claim 10 further comprising a closure in communication with the conductor, the closure including one or more of a conductive adhesive, a conductive closure mechanism, a magnetic closure mechanism, a conductive rivet or staple, a crimped material, or a heat-bonded material in proximity to the conductor.
- 15
- ✓ 12. The identification appliance of claim 11 wherein after the closure is closed, the control circuit is adapted to determine whether the closure has been opened or tampered with.
- 20
- ✕ 13. The identification appliance of claim 9 wherein the first contact and the second contact comprise first and second conductors, the closure of the fastener connecting the first and second conductors to enable at least one electrical circuit.
- 25
- ✕ 14. The identification appliance of claim 9 wherein the first contact and the second contact comprise first and second conductors, the closure of the fastener altering a capacitance between the first and second conductors, which enables an electrical circuit.
- 30
- ✓ 15. The identification appliance of claim 1 wherein the information includes biometric data.
- ✕ 16. The identification appliance of claim 14 wherein the biometric data includes a retina, fingerprint, iris, voice, or genetic characteristic of the person.
- ✓ 17. The identification appliance of claim 1 wherein the information includes an image of a feature of the person.
- ✓ 18. The identification appliance of claim 1 wherein the information include

- optical character recognizable data.
- ✓ 19. The identification appliance of claim 1 wherein the identification appliance is a wristband, headband, armband, ankleband, neckband, or legband.
- 5 ✓ 20. The identification appliance of claim 1 wherein the identification appliance is a patch or card.
- ✓ 21. The identification appliance of claim 1 wherein at least a circuit component of the circuit is formed substantially of at least one organic material.
- 10 ✓ 22. The identification appliance of claim 21 wherein the circuit is formed entirely of at least one organic material.
- ✓ 23. The identification appliance of claim 1 further comprising a power source coupled to supply power to the circuit, the power source being formed at least partially of an organic material.
- 15 ✓ 24. The identification appliance of claim 1 further comprising a diode within the circuit, the diode comprising an organic material.
- ✓ 25. The identification appliance of claim 1 further comprising a data storage device adapted to store the information, the data storage device formed substantially of at least one organic material.
- 20 ✓ 26. The identification appliance of claim 25 further comprising a keypad coupled to the data storage device, the keypad adapted to input data into the data storage device.
- ✓ 27. The identification appliance of claim 1 further comprising a microstrip antenna coupled to the circuit, the antenna being adapted to transmit the information to a device external to the identification appliance.
- 25 ✓ 28. The identification appliance of claim 27 wherein the microstrip antenna is a continuous radiator.
- ✓ 29. The identification appliance of claim 27 wherein the microstrip antenna is disposed on or in the structure such that when the structure is worn by or attached to the person, the microstrip antenna is adapted to radiate energy
- 30

away from the person and to radiate substantially less energy toward the person.

- 5 ✓ 30. The identification appliance of claim 27 wherein the microstrip antenna comprises a conductive patch layer, a conductive ground layer and a dielectric material disposed between the patch layer and the ground layer, the ground layer being located closer to the person than the patch layer when the structure is worn by or attached to the person.
- 10 ✓ 31. The identification appliance of claim 1 further comprising an audio or visual display coupled to the circuit.
- ✓ 32. The identification appliance of claim 1 wherein the information includes medical data about the person.
- ✓ 33. **[[FIG. 3]]** The identification appliance of claim 1 wherein the circuit is adapted to disable a circuit function if the circuit detects that the identification appliance has been tampered with.
- 15 ✓ 34. The identification appliance of claim 1 further comprising a data storage device adapted to store the information about the person and the circuit is adapted to alter, erase, or damage the information if the circuit determines that the identification appliance has been tampered with.
- 20 ✓ 35. The identification appliance of claim 34 wherein the data storage device is a memory and the circuit is adapted to alter, erase, or damage the information in the memory if the circuit determines that the identification appliance has been tampered with.
- 25 ✓ 36. The identification appliance of claim 34 wherein the circuit is adapted to permit an authorized person or agency to remove the identification appliance without the circuit altering, erasing, or damaging the information in the data storage device.
- ✓ 37. **[[FIG. 4]]** The identification appliance of claim 1 wherein the circuit is adapted to disable or change a circuit function if the circuit determines that the identification appliance has been detached from the person.
- 30 ✓ 38. The identification appliance of claim 37 wherein the circuit function is the

- communication of the information external to the identification appliance.
- ✓39. The identification appliance of claim 37 wherein the circuit function includes the supply of power to the circuit.
- ✓40. The identification appliance of claim 37 wherein the circuit function includes the enablement of an antenna.
- 5 ✓41. The identification appliance of claim 37 wherein the circuit function includes the tuning of an antenna.
- ✓42. The identification appliance of claim 37 wherein the circuit function includes changing a logic state input to the circuit.
- 10 ✓43. The identification appliance of claim 37 further comprising an electrical conductor disposed in or on the structure, the conductor comprising one or more of a conductive wire or fiber, a conductive foil, a meltable conductor, or a conductor printed on the structure, the severing or breaking of the conductor causes the circuit to determine that tampering or opening of the fastener occurred.
- 15 ✓44. The identification appliance of claim 43 further comprising a closure in communication with the conductor, the closure including one or more of a conductive adhesive, a conductive closure mechanism, a magnetic closure mechanism, a conductive rivet or staple, a crimped material, or a heat-bonded material in proximity to the conductor.
- 20 ✓45. The identification appliance of claim 37 further comprising a pattern of non-conductive fibers embedded within the structure, the fibers disabling, shorting, or breaking an electrical circuit when the identification appliance is overly stretched or twisted.
- 25 ✓46. The identification appliance of claim 45 wherein the disabling, shorting, or breaking of the electrical circuit prevents the identification appliance from transmitting the information external to the identification appliance.
- ✓47. The identification appliance of claim 45 wherein the disabling, shorting, or breaking of the electrical circuit disable a data storage device, the data storage device storing the information.
- 30

- ✓ 48. **[[FIG. 5]]** The identification appliance of claim 1 further comprising an indicator, the indicator adapted to indicate whether the identification appliance has been tampered with.
- 5 ✓ 49. The identification appliance of claim 48 wherein the indicator comprises an ink or dye, the indicator adapted to release the ink or dye when the circuit detects tampering with the identification appliance.
- ✓ 50. **[[FIG. 6]]** The identification appliance of claim 1 further comprising an indicator, the indicator adapted to indicate whether the fastener is closed.
- 10 ✓ 51. The identification appliance of claim 50 wherein the indicator forms a visible identifying pattern when the fastener is closed.
- ✓ 52. The identification appliance of claim 51 wherein the circuit is adapted to enable an electrical circuit corresponding to the identifying pattern.
- 15 ✓ 53. **[[BIOMETRICS: FIG. 7]]** An identification appliance adapted to provide information about a person, the identification appliance comprising:
- a structure adapted to be worn by or attached to the person;
- a communication circuit disposed in or on the structure, the circuit adapted to receive biometric information about the person from a source external to the identification appliance; and
- 20 a data storage device adapted to store the biometric information.
- ✓ 54. **[[FIG. 8]]** The identification appliance of claim 53 wherein the communication circuit includes an input port adapted to be coupled to an external device, the external device being adapted to transmit the biometric information to the communication circuit through the input port.
- 25 ✓ 55. The identification appliance of claim 54 wherein the communication circuit is adapted to be coupled to a second external device, the second external device being adapted to transmit second information about the person to the communication circuit, the data storage device adapted to store the biometric information and the second information.
- 30 ✓ 56. The identification appliance of claim 53 wherein the data storage device

includes a memory.

✓ 57. The identification appliance of claim 56 wherein the memory is non-volatile.

✓ 58. The identification appliance of claim 53 further comprising a fastener adapted to attach the structure to the person; and a circuit disposed in or on the structure, the closing of the fastener enables a circuit function.

✓ 59. The identification appliance of claim 58 wherein the circuit function is the communication of the information about the person externally of the identification appliance.

✓ 60. The identification appliance of claim 58 wherein the circuit function includes the supply of power to the circuit.

✓ 61. The identification appliance of claim 58 wherein the circuit function includes the enablement of an antenna.

✓ 62. The identification appliance of claim 58 wherein the circuit function includes the tuning of an antenna.

✓ 63. The identification appliance of claim 58 wherein the circuit function includes changing a logic state input to the circuit.

✓ 64. The identification appliance of claim 53 wherein the biometric information includes a retina, fingerprint, iris, voice, or genetic characteristic of the person.

✓ 65. The identification appliance of claim 53 wherein the biometric information includes an image of the person.

✓ 66. The identification appliance of claim 53 wherein the biometric information include optical character recognizable data.

✓ 67. The identification appliance of claim 53 wherein the identification appliance is a wristband, headband, armband, ankleband, neckband, or legband.

✓ 68. The identification appliance of claim 53 wherein the identification appliance is a patch or card.

- ✓ 69. The identification appliance of claim 53 wherein at least a component of the circuit is formed substantially of at least one organic material.
- ✓ 70. The identification appliance of claim 69 wherein the circuit is formed entirely of at least one organic material.
- 5 ✓ 71. The identification appliance of claim 53 further comprising a power source coupled to supply power to the circuit, the power source being formed at least partially of an organic material.
- ✓ 72. The identification appliance of claim 53 further comprising a diode within the circuit, the diode comprising an organic material.
- 10 ✗ 73. The identification appliance of claim 53 further comprising a data storage device adapted to store the information, the data storage device formed substantially of at least one organic material.
- ✓ 74. The identification appliance of claim 53 further comprising a microstrip antenna coupled to the circuit, the antenna being adapted to transmit the information to a device external to the identification appliance.
- 15 ✓ 75. **[[FIG. 9]]** The identification appliance of claim 58 wherein the circuit is adapted to disable a circuit function if the circuit detects that the identification appliance has been tampered with.
- ✓ 76. The identification appliance of claim 75 wherein the circuit function is the communication of the information externally of the identification appliance.
- 20 ✓ 77. The identification appliance of claim 75 further comprising a data storage device adapted to store the information about the person and the circuit is adapted to alter, erase, or damage the information if the circuit determines that the identification appliance has been tampered with.
- 25 ✓ 78. The identification appliance of claim 77 wherein the data storage device is a memory and the circuit is adapted to alter, erase, or damage the information in the memory if the circuit determines that the identification appliance has been tampered with.
- 30 ✓ 79. The identification appliance of claim 77 wherein the data storage device is

adapted to store the biometric information and an associated information about the person.

- ✓ 80. **[[method of using FIG. 8]]** A method of verifying whether the possessor of an identification appliance is its authorized bearer, the method comprising:
- 5 retrieving biometric data of the bearer which was previously stored in a circuit in the identification appliance;
- obtaining current biometric data from the possessor of the identification appliance;
- 10 determining if the previously-stored biometric data and the current biometric data are associated with the same person;
- retrieving associated data of the bearer which was previously stored in the circuit in the identification appliance;
- 15 obtaining current associated data from the possessor of the identification appliance; and
- determining if the previously-stored associated data and the current associated data are from the same person.
- ✓ 81. The method of claim 80 further comprising indicating whether the identity of the authorized bearer has been verified.
- 20 ✓ 82. The method of claim 81 wherein the indicating step comprises indicating in an audible, visual, or vibrating manner which is perceptible to a human.
- ✓ 83. The method of claim 80 further comprising displaying the previously-stored biometric data.
- 25 ✗ 84. The method of claim 80 further comprising displaying the previously-stored biometric data and the previously-stored associated data.
- ✗ 85. The method of claim 80 wherein the step of obtaining current biometric data includes connecting a device to the identification appliance, the device being adapted to obtain current biometric data of the possessor of the identification appliance.
- 30 ✗ 86. The method of claim 85 wherein the step of obtaining current associated

data includes connecting a second device to the identification appliance,
the second device being adapted to obtain current associated data of the
possessor of the identification appliance.

- 5 × 87. **[[VARIOUS SENSORS]]** An identification appliance adapted to provide
information about a person, the identification appliance comprising:
a structure adapted to be worn by or attached to the person;
a circuit disposed in or on the structure;
a sensor coupled to the circuit, the sensor being adapted to receive information
about the person from a source external to the identification appliance; and
10 a data storage device adapted to store the information.
- ? 88. **[[MORE BIOMETRIC SENSORS]]** The identification appliance of
claim 87 wherein the sensor includes a biometric sensor adapted to receive
biometric information about the person.
- ? 89. The identification appliance of claim 88 wherein the biometric
15 information includes a retina, fingerprint, iris, voice, or genetic
characteristic of the person.
- ? 90. The identification appliance of claim 88 wherein the biometric
information includes an image of the person.
- ? 91. The identification appliance of claim 88 wherein the biometric
20 information include optical character recognizable data.
- ? 92. The identification appliance of claim 88 wherein the biometric sensor
includes a light-emitting device adapted to emit light towards the person
and a light-sensing device adapted to measure light reflection off the
person to obtain a fingerprint characteristic.
- ? 93. The identification appliance of claim 88 wherein the biometric sensor
25 includes a light-emitting device adapted to emit light towards the person
and a light-sensing device adapted to measure light reflection off the
person to obtain a retinal characteristic.
- ? 94. The identification appliance of claim 88 wherein the biometric sensor is
30 formed of at least one organic material.

- 7
- 5
- 10
- 15
- 20
- 25
- 30
95. The identification appliance of claim 87 wherein the identification appliance is a wristband, headband, armband, ankleband, neckband, or legband.
96. The identification appliance of claim 87 wherein the identification appliance is a patch or card.
97. **[[ACOUSTIC SENSORS – FIG. 22]]** The identification appliance of claim 87 wherein the sensor includes an acoustic sensor adapted to receive acoustic information about the person.
98. The identification appliance of claim 97 wherein the acoustic sensor is adapted to receive speech information from the person and the circuit is adapted to process the speech information.
99. The identification appliance of claim 98 wherein the circuit is adapted to derive a unique identifying information about the person from the speech information.
100. The identification appliance of claim 98 wherein the circuit includes an audio generation circuit adapted to output synthesized speech.
101. The identification appliance of claim 97 wherein the acoustic sensor comprises a piezoelectric transducer.
102. The identification appliance of claim 97 wherein the acoustic sensor is formed substantially of at least one organic material.
103. **[[OPTICAL SENSORS – FIG. 24]]** The identification appliance of claim 87 wherein the sensor includes an optical sensor adapted to receive information about the person optically.
104. The identification appliance of claim 103 wherein the optical sensor comprises a light detector adapted to capture images of the person's face, fingerprint, iris, or retina.
105. The identification appliance of claim 104 wherein the optical sensor includes a charge coupled device.
106. The identification appliance of claim 104 wherein the optical sensor includes a photodetector.

107. The identification appliance of claim 103 wherein the optical sensor is formed of at least one organic material.
108. **[[CHEMICAL SENSORS]]** The identification appliance of claim 87 wherein the sensor includes a chemical sensor adapted to receive the information about the person chemically.
109. The identification appliance of claim 108 wherein the chemical sensor is adapted to assay the biochemical content of the person's scent, blood, or breath.
110. **[[HUMIDITY SENSORS]]** The identification appliance of claim 87 wherein the sensor includes a humidity sensor adapted to receive information about the humidity.
111. **[[HEAT SENSORS]]** The identification appliance of claim 87 wherein the sensor includes a heat sensor adapted to receive temperature information.
112. **[[PRESSURE SENSORS]]** The identification appliance of claim 87 wherein the sensor includes a pressure sensor adapted to receive pressure information.
113. **[[ELECTRO-MAGNETIC SENSORS]]** The identification appliance of claim 87 wherein the sensor includes an electro-magnetic sensor adapted to receive electro-magnetic energy.
114. The identification appliance of claim 87 wherein the sensor is formed of at least one organic material.
115. The identification appliance of claim 87 further comprising an indicator adapted to provide an audible, visual, or vibrating indication to a human.
116. The identification appliance of claim 87 further comprising a keypad coupled to the data storage device, the keypad adapted to input information into the data storage device.
117. The identification appliance of claim 87 further comprising a microstrip antenna coupled to the circuit, the antenna being adapted to transmit the information to a device external to the identification appliance.

- 3
1
- 5
- 10
- 15
- 20
- 25
- 30
- 7
- ↑
118. The identification appliance of claim 116 wherein the microstrip antenna is disposed on or in the structure such that when the structure is worn by or attached to the person, the microstrip antenna is adapted to radiate energy away from the person and to radiate substantially less energy toward the person.
119. The identification appliance of claim 87 further comprising a power source coupled to supply power to the circuit, the power source being formed at least partially of an organic material.
120. The identification appliance of claim 118 wherein the power source includes a photovoltaic cell.
121. The identification appliance of claim 118 wherein the power source includes a button-style battery.
122. The identification appliance of claim 87 further comprising a diode within the circuit, the diode comprising an organic material.
123. The identification appliance of claim 87 wherein the data storage device is formed substantially of at least one organic material.
124. The identification appliance of claim 87 wherein the data storage device includes a non-volatile memory adapted to store the information about the person.
125. The identification appliance of claim 87 wherein the information about the person stored in an encrypted form in the data storage device.
- ✓ 126. The identification appliance of claim 53 wherein the information about the person stored in an encrypted form in the data storage device.
- ✓ 127. **[[READER/VERIFIER: FIGS 33-34]]** A method of verifying whether the possessor of an identification appliance is its authorized bearer, the identification appliance containing a first set of encoded data about the bearer, the method comprising:
- a) obtaining a second set of data about the possessor of the identification appliance;
- b) encoding the set of data to obtain a second set of encoded data;

- c) communicating the first set of encoded data stored in the identification appliance to a reader; and
 - d) determining whether the first and second sets of encoded data are those of the same person.
- 5 ✓128. The method of verifying of claim 127 wherein the first and second sets of encoded data include biometric information.
- ✓129. The method of verifying of claim 127 wherein the determining step determines the number of characteristics of the first and second set of encoded data that match.
- 10 ✓130. The method of verifying of claim 129 wherein the determining step determines there is a high probability of a match if the number of characteristics of the first and second set of encoded data that match is high and there is a low probability of a match if the number of characteristics of the first and second set of encoded data that match is
- 15 low.
- ✓131. The method of verifying of claim 129 wherein the determining step compares the number of matching characteristics to a threshold number to determine the probability that the first and second sets of encoded data are from the same person.
- 20 ✓132. The method of verifying of claim 127 further comprising assigning a weight to each data in the first or second sets of encoded data based on the data's effect on the overall probability of identity verification.
- ✓133. The method of verifying of claim 127 further comprising indicating the result of whether the first and second sets of encoded data are determined
- 25 to be those of the same person.
- ✓134. The method of verifying of claim 127 further comprising indicating data from the first and second sets of encoded data which do not match.
- ✓135. The method of verifying of claim 134 further comprising permitting a human to determine whether the data from the first and second sets of
- 30 encoded data match and to input the decision.

- ✓ 136. The method of verifying of claim 134 further comprising preventing the possessor from gaining access to a restricted area if the determining step determines that the first and second sets of encoded data are not from the same person.
- 5 ✓ 137. **[[BUCKLE]]** The identification appliance of claim 1 wherein the fastener comprises a buckle attached to the structure, the buckle adapted to adjustably secure the structure to the person.
- ✓ 138. The identification appliance of claim 137 further comprising a dye reservoir in communication with the buckle which releases a dye from the dye reservoir when the buckle is tampered with.
- 10 ✓ 139. The identification appliance of claim 137 wherein the buckle comprises an electrical conductor coupled to the circuit, the closing of the buckle enables a function of the circuit.
- ✓ 140. The identification appliance of claim 137 wherein the buckle comprises an electrical conductor coupled to the circuit, the opening of the buckle disables a function of the circuit.
- 15 ✓ 141. The identification appliance of claim 139 wherein the buckle is formed of an organic material having an electrically conductive coating.
- ✓ 142. **[[AIRLINE TICKETING: FIG. 10]]** A method of passenger ticketing and boarding of a vehicle, the method comprising:
- 20 (a) at check-in,
- (i) storing identifying data about a passenger in an identification band; and
- (ii) attaching the identification band to the passenger; and
- 25 (b) at boarding,
- (i) receiving the stored identifying data in the identification band on the passenger; and
- (ii) processing the received identifying data to verify the passenger's identity.
- 30 ✓ 143. The method of claim 142 wherein the storing step stores the identifying

data in the identification band, where the identification band is a wristband, headband, armband, neckband, ankleband, or legband.

- 5 ✓144. The method of claim 142 wherein the storing step stores the identifying data, the identifying data comprising a retina, fingerprint, iris, voice, or genetic characteristic of the passenger.
- ✓145. The method of claim 142 further comprising obtaining an image of a feature of the passenger.
- ✓146. The method of claim 142 wherein the storing step stores the identifying data in a form of character recognizable data.
- 10 ✓147. The method of claim 142 wherein the storing step encodes the identifying data prior to storing the data.
- ✓148. The method of claim 142 wherein the storing step encrypts the identifying data prior to storing the data.
- ✓149. The method of claim 142 wherein the storing step stores the identifying data in a nonvolatile memory in the identification band.
- 15 ✓150. The method of claim 142 wherein the processing step determines whether the identification band has been opened or tampered with.
- ✓151. The method of claim 142 wherein the storing step includes obtaining current identifying data about the passenger.
- 20 ✓152. The method of claim 142 further comprising displaying the received identifying data.
- ✓153. The method of claim 142 wherein the receiving step receives the stored identifying data by wireless communication with the identification band.
- ✓154. The method of claim 142 further comprising configuring the identification band to expire automatically upon an event.
- 25 ✓155. The method of claim 154 wherein the event is the boarding of the passenger onto the vehicle.
- ✓156. The method of claim 142 wherein the vehicle is an airplane.
- ✓157. The method of claim 142 wherein the vehicle is a boat.
- 30 ✓158. The method of claim 142 wherein the vehicle is a train.

- ✓159. The method of claim 142 wherein the vehicle is a bus.
- ✓160. The method of claim 142 further comprising monitoring the location of the passenger.
- ✓161. **[[FIG. 11]]** A method of securely tagging and claiming passenger baggage for a vehicle, the method comprising:
- 5 (a) at departure,
- (i) storing identifying data about a passenger in an identification band;
- (ii) attaching an identification band to the passenger; and
- 10 (iii) attaching an identification band to each item of the passenger's checked baggage; and
- (b) at baggage claim,
- (i) receiving the stored identifying data in the identification band on the passenger;
- 15 (ii) receiving the stored identifying data in the identification band on each item of the claimed baggage; and
- (iii) processing the received identifying data to verify that each item of the claimed baggage is associated with the passenger.
- 20 ✓162. The method of claim 161 wherein the storing step stores the identifying data in the identification band, where the identification band is a wristband, headband, armband, neckband, ankleband, or legband.
- ✓163. The method of claim 161 wherein the storing step stores the identifying data, the identifying data comprising a retina, fingerprint, iris, voice, or genetic characteristic of the passenger.
- 25 ✓164. The method of claim 161 further comprising obtaining an image of a feature of the passenger.
- ✓165. The method of claim 161 wherein the storing step stores the identifying data in a form of character recognizable data.
- 30 ✓166. The method of claim 161 wherein the storing step encodes the identifying

data prior to storing or transmitting the data.

✓ 167. The method of claim 161 wherein the storing step encrypts the identifying data prior to storing or transmitting the data.

✓ 168. The method of claim 161 wherein the storing step stores the identifying data in a nonvolatile memory in the identification band.

✓ 169. The method of claim 161 wherein the processing step determines whether the identification band has been opened or tampered with.

✓ 170. The method of claim 161 wherein the storing step includes obtaining current identifying data about the passenger.

10 ✓ 171. The method of claim 161 further comprising displaying the received identifying data.

✓ 172. The method of claim 161 wherein the receiving step receives the stored identifying data by wireless communication with the identification band.

15 ✓ 173. The method of claim 161 further comprising configuring the identification band to expire automatically upon an event.

✓ 174. The method of claim 173 wherein the event is the boarding of the passenger onto the vehicle.

✓ 175. The method of claim 161 wherein the vehicle is an airplane.

✓ 176. The method of claim 161 wherein the vehicle is a boat.

20 ✓ 177. The method of claim 161 wherein the vehicle is a train.

✓ 178. The method of claim 161 wherein the vehicle is a bus.

✓ 179. The method of claim 161 further comprising monitoring the location of the passenger.

25 ✓ 180. The method of claim 161 further comprising verifying the identity of the passenger at a security checkpoint.

✓ 181. The method of claim 161 further comprising updating the identification band of the passenger and the identification band on the passenger's checked baggage if the itinerary of the passenger or the passenger's checked baggage changes.

30 ✓ 182. **[[Green card]]** The method of associating an immigration status with a

person, the method comprising:
determining the immigration status of the person for a country of interest;
storing the immigration status and an identifying data about the person in
an identification appliance; and
providing the identification appliance to the person.

5

✓183. The method of claim 182 wherein the storing step stores the identifying
data in the identification appliance, where the identification appliance is a
wristband, headband, armband, ankleband, neckband, or legband.

10

✓184. The method of claim 182 wherein the storing step stores the identifying
data, the identifying data comprising a retina, fingerprint, iris, voice, or
genetic characteristic of the person.

✓185. The method of claim 182 further comprising obtaining an image of a
feature of the person.

15

✓186. The method of claim 182 wherein the storing step stores the identifying
data in a form of character recognizable data.

✓187. The method of claim 182 wherein the storing step encodes the identifying
data prior to storing or transmitting the data.

✓188. The method of claim 182 wherein the storing step encrypts the identifying
data prior to storing or transmitting the data.

20

✓189. The method of claim 182 wherein the storing step stores the identifying
data in a nonvolatile memory in the identification appliance.

✓190. The method of claim 182 wherein the processing step determines whether
the identification appliance has been opened or tampered with.

25

✓191. The method of claim 182 wherein the storing step includes obtaining
current identifying data about the person.

✓192. The method of claim 182 further comprising verifying the immigration
status of the person when the person is seeking entry into the country.

✓193. The method of claim 182 further comprising mailing the identification
appliance to the person.

30

✓194. The identification appliance of claim 48 wherein the indicator is adapted

- to release a substance perceptible to an animal.
- 5 ✓ 195. The identification appliance of claim 48 wherein the indicator is adapted to release a substance perceptible to a machine.
- ✗ 196. The identification appliance of claim 87 further comprising an indicator which is adapted to release a substance perceptible to an animal.
- ✗ 197. The identification appliance of claim 87 further comprising an indicator which is adapted to release a substance perceptible to a machine.
- ✗ 198. The identification appliance of claim 138 further comprising an indicator which is adapted to release a substance perceptible to an animal.
- 10 ✗ 199. The identification appliance of claim 138 further comprising an indicator which is adapted to release a substance perceptible to a machine.
- ✓ 200. The identification appliance of claim 53 wherein the communication circuit is adapted to transmit information about the person in an encrypted form.
- 15 ✗ 201. The identification appliance of claim 87 wherein the circuit is adapted to transmit information about the person in an encrypted form.
- ✓ 202. The identification appliance of claim 139 wherein the buckle is formed of an organic material which is electrically conductive.
- 20 ✓ 203. **[[MIX AND MATCHES VARIOUS TYPES OF SENSORS WITH EACH OTHER (e.g., biometric with acoustic, biometric with optical, etc)]** The identification appliance of claim 1 further comprising an acoustic sensor adapted to receive acoustic information about the person.
- ✓ 204. The identification appliance of claim 203 wherein the acoustic sensor is adapted to receive speech information from the person and the circuit is adapted to process the speech information.
- 25 ✓ 205. The identification appliance of claim 15 further comprising an acoustic sensor adapted to receive acoustic information about the person.
- ✓ 206. The identification appliance of claim 1 further comprising an optical sensor adapted to receive information about the person optically.
- 30 ✓ 207. The identification appliance of claim 206 wherein the optical sensor

comprises a light detector adapted to capture images of the person's face, fingerprint, iris, or retina.

- ✓ 208. The identification appliance of claim 15 further comprising an optical sensor adapted to receive information about the person optically.
- 5 ✓ 209. The identification appliance of claim 1 further comprising a chemical sensor adapted to receive the information about the person chemically.
- ✓ 210. The identification appliance of claim 209 wherein the chemical sensor is adapted to assay the biochemical content of the person's scent, blood, or breath.
- 10 ✓ 211. The identification appliance of claim 15 further comprising a chemical sensor adapted to receive the information about the person chemically.
- ✓ 212. The identification appliance of claim 53 further comprising an acoustic sensor adapted to receive acoustic information about the person.
- ✓ 213. The identification appliance of claim 212 wherein the acoustic sensor is adapted to receive speech information from the person and the communication circuit is adapted to process the speech information.
- 15 ✓ 214. The identification appliance of claim 53 further comprising an optical sensor adapted to receive information about the person optically.
- ✓ 215. The identification appliance of claim 214 wherein the optical sensor comprises a light detector adapted to capture images of the person's face, fingerprint, iris, or retina.
- 20 ✓ 216. The identification appliance of claim 53 further comprising a chemical sensor adapted to receive the information about the person chemically.
- ✓ 217. The identification appliance of claim 216 wherein the chemical sensor is adapted to assay the biochemical content of the person's scent, blood, or breath.
- 25 ✓ 218. The identification appliance of claim 88 further comprising an acoustic sensor adapted to receive acoustic information about the person.
- ✓ 219. The identification appliance of claim 88 further comprising an optical sensor adapted to receive information about the person optically.
- 30

- ✓ 220. The identification appliance of claim 88 further comprising a chemical sensor adapted to receive the information about the person chemically.
- ✓ 221. The identification appliance of claim 103 further comprising an biometric sensor adapted to receive biometric information about the person.
- 5 ✓ 222. The identification appliance of claim 103 further comprising an acoustic sensor adapted to receive acoustic information about the person.
- ✓ 223. The identification appliance of claim 103 further comprising a chemical sensor adapted to receive the information about the person chemically.
- 10 ✗ 224. The identification appliance of claim 108 further comprising an biometric sensor adapted to receive biometric information about the person.
- ✗ 225. The identification appliance of claim 108 further comprising an acoustic sensor adapted to receive acoustic information about the person.
- ✗ 226. The identification appliance of claim 108 further comprising an optical sensor adapted to receive the information about the person optically.
- 15 ✗ 227. The identification appliance of claim 113 further comprising an biometric sensor adapted to receive biometric information about the person.
- ✗ 228. The identification appliance of claim 113 further comprising an acoustic sensor adapted to receive acoustic information about the person.
- ✗ 229. The identification appliance of claim 113 further comprising an optical sensor adapted to receive the information about the person optically.
- 20 ✗ 230. The identification appliance of claim 113 further comprising a chemical sensor adapted to receive the information about the person chemically.
- ✓ 231. The method of claim 127 wherein the second set of data includes biometric information about the possessor.
- 25 ✓ 232. The method of claim 127 wherein the second set of data includes acoustic information about the possessor's voice or speech characteristic.
- ✓ 233. The method of claim 127 wherein the second set of data includes optical information about the possessor.
- ✓ 234. The method of claim 127 wherein the second set of data includes chemical information about the possessor.
- 30

- ✓ 235. The method of claim 127 wherein the second set of data includes genetic information about the possessor.

ABSTRACT

An enhanced identification appliance, such as a wristband, bracelet, patch, headband, neckband, ankleband, legband, card, sticker, or other wearable appliance, may have a biometric sensor, chemical sensor, optical sensor, heat sensor, pressure sensor, humidity sensor, electromagnetic sensor, acoustic sensor, various opto-electronics and/or various security features such as tamper-evident and tamper-resistant features. The sensors may obtain information about the wearer such as a fingerprint, retina, iris, blood, DNA, genetic data, voice pattern, temperature and other characteristic. Security features include a fastener on the identification appliance, which indicates whether the appliance has been attached to a wearer and if so, enables circuit functions. If one tampers with the appliance, circuit functions may be disabled, certain data erased, and/or evidence of tampering made apparent. The appliance may monitor the location or determine the identity of passengers for an airplane, train, boat, bus, or other vehicle. Alternatively, the identification band may contain a person's immigration status.

Version I

LYON & LYON LLP
A LIMITED LIABILITY PARTNERSHIP
INCLUDING PROFESSIONAL CORPORATIONS
1900 Main Street, Sixth Floor
Irvine, California 92614
Phone: (949) 567-2300
Fax: (949) 567-6600

FACSIMILE TRANSMITTAL FORM

| | | |
|---|---|--|
| To: Dr. Walter W. Mosher, President Precision Dynamics Corporation | Fax Number: (818) 897-7871 | Phone Number: (818) 897-1111 |
| From: David E. Wang | Fax Number: 949-567-6600 | Phone Number: 949-567-2300 |
| Re: WRISTBAND WITH BIOMETRIC FUNCTIONS | Date/Time sent: 3/7/02 4:46 PM. | No. of Pages: 17 (incl. cover) |
| Client Name: PRECISION DYNAMICS | Client Matter No.: L&L Docket No. 269/223 | |

If you do not receive all of the pages, please call Valerie Cloyd at (949) 567-2300, extension 1146.

Notes/Comments:

Attached are the drawings that go with the draft specification that I emailed today.

TO BE COMPLETED BY FAX OPERATOR

TIME TRANSMITTED: _____ TRANSMITTED BY: _____

This transmittal is intended only for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this transmittal is not the intended recipient or the employee or agent responsible for delivering the transmittal to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone, and return the original message to us by mail at the above address. Thank you.

OC-94216.1

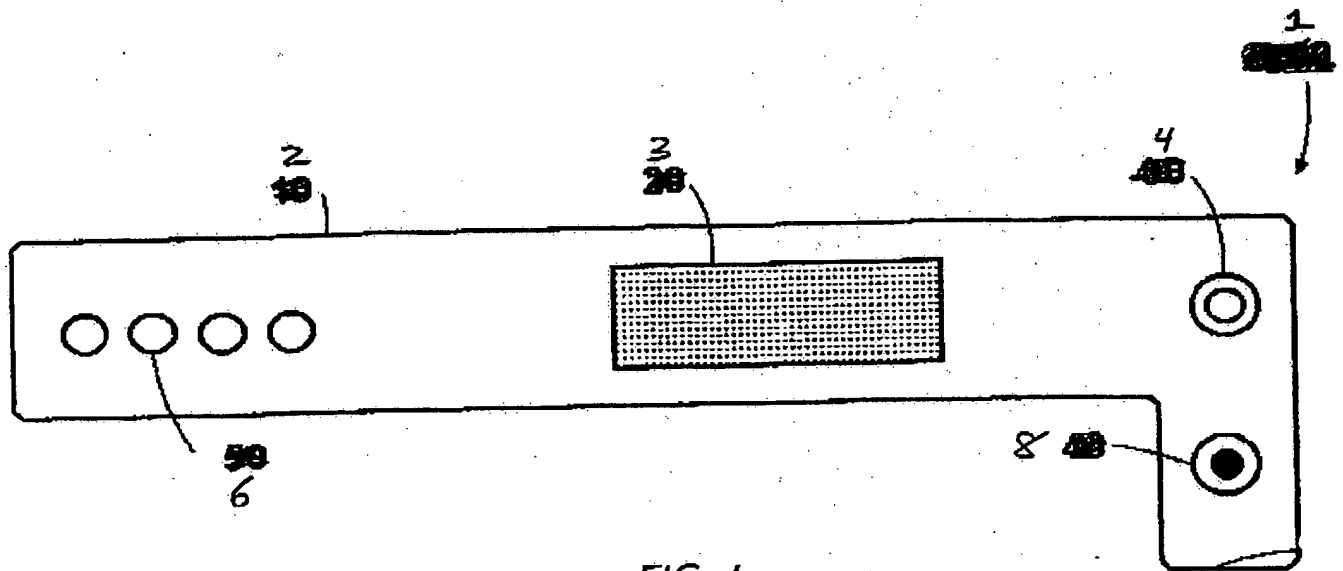


FIG. 1
PRIOR ART

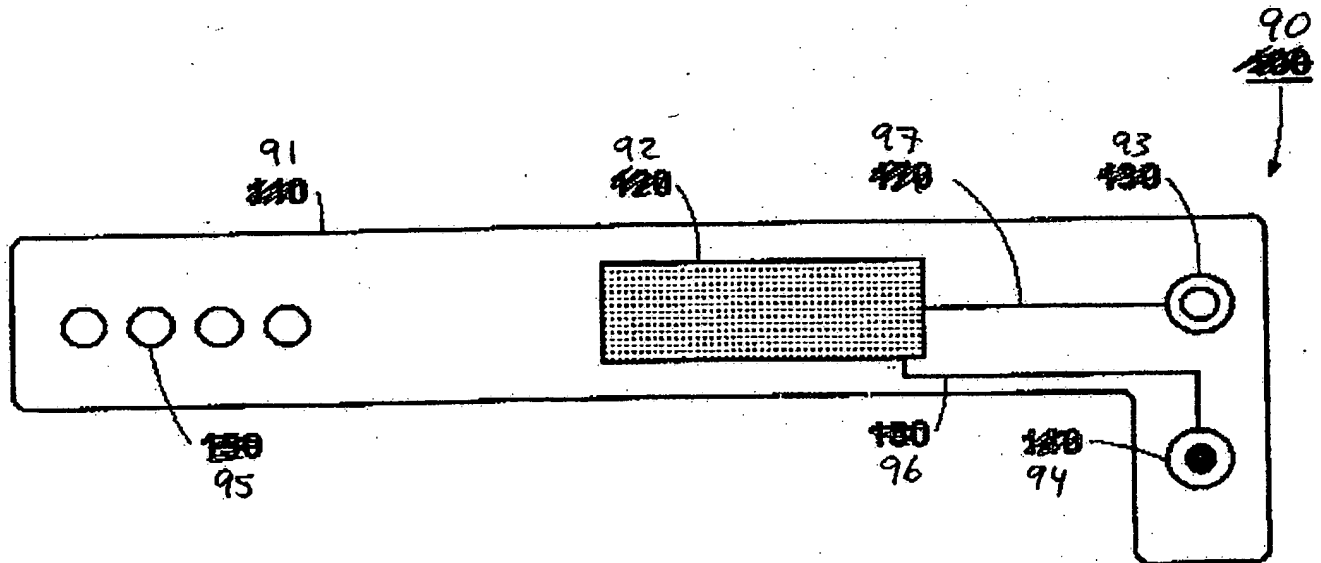
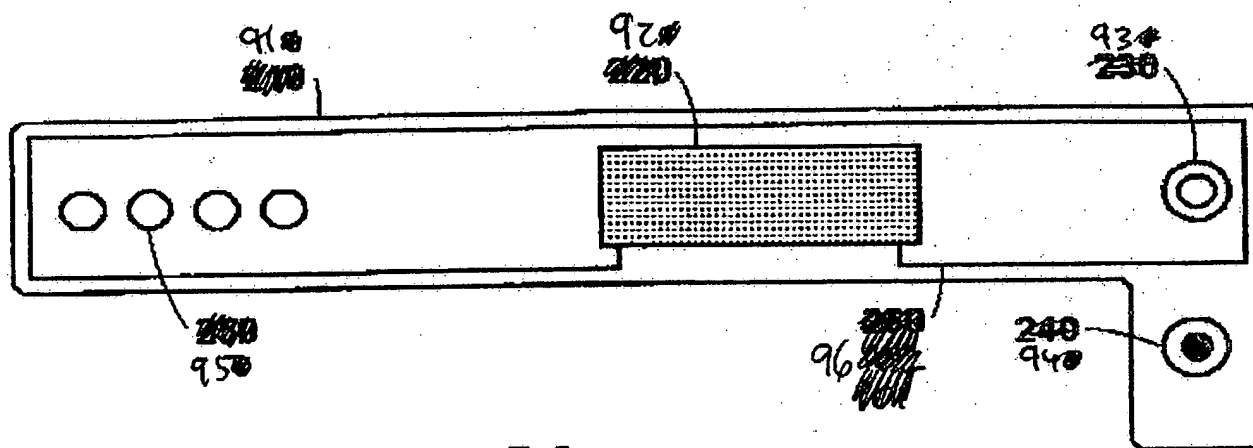
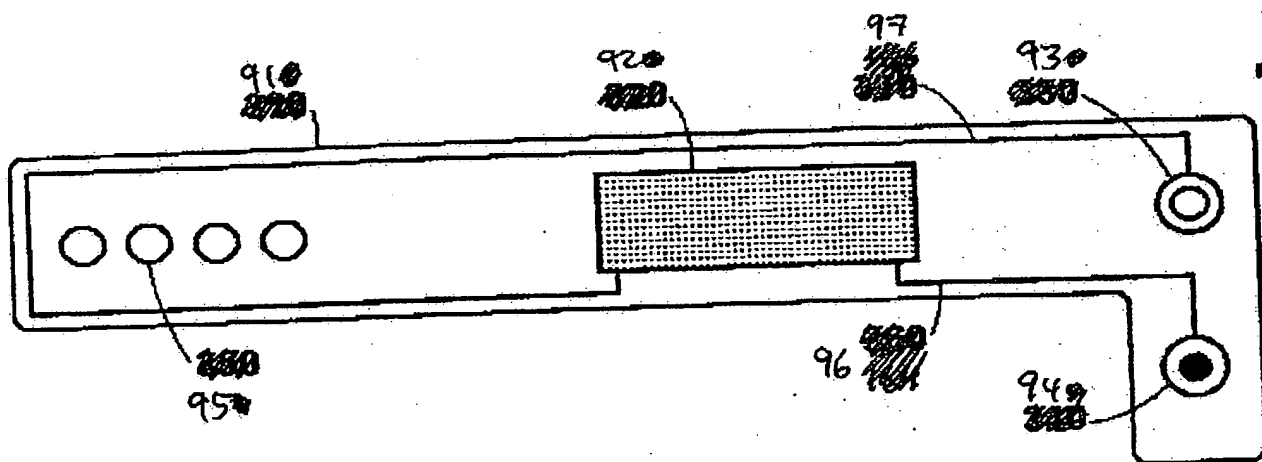


FIG. 2

90 ~~100~~
~~200~~



90 ~~100~~
~~300~~



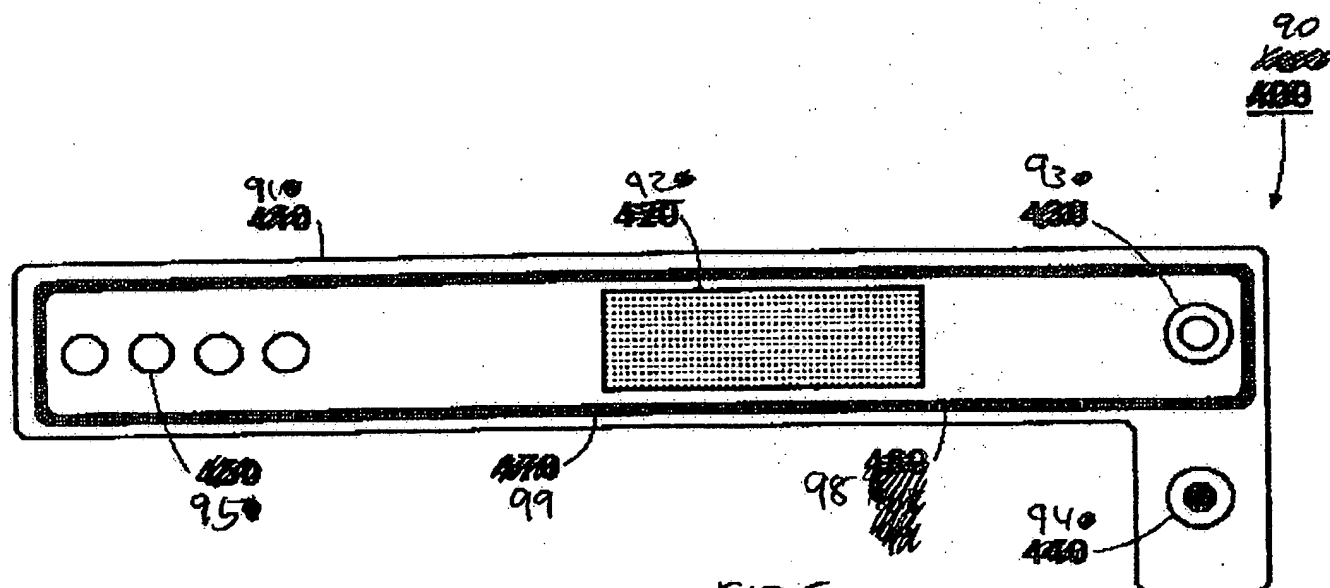


FIG.5

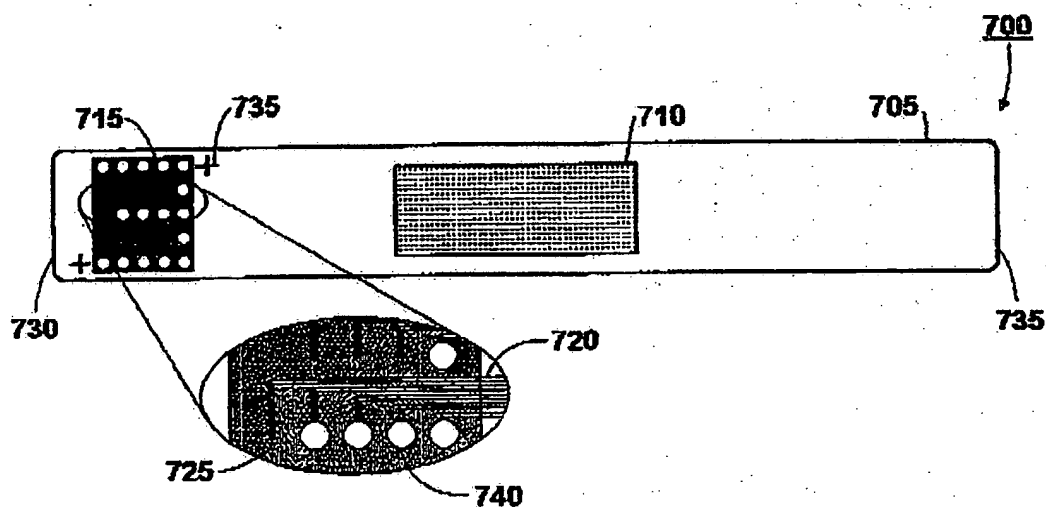


FIG. 6

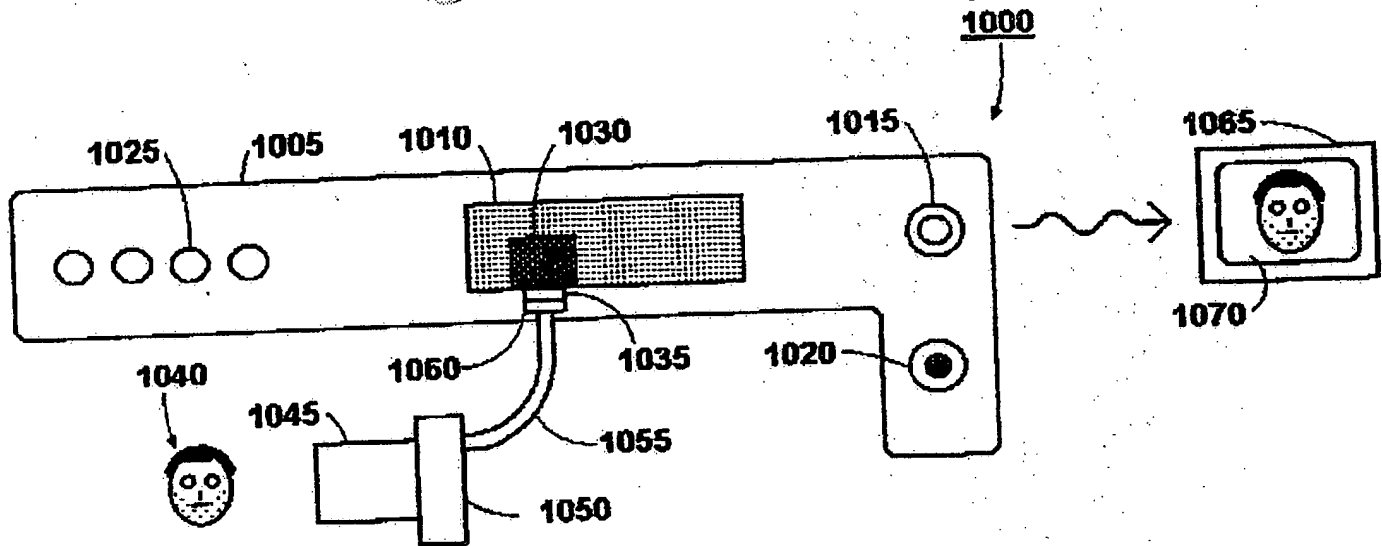


FIG. 7

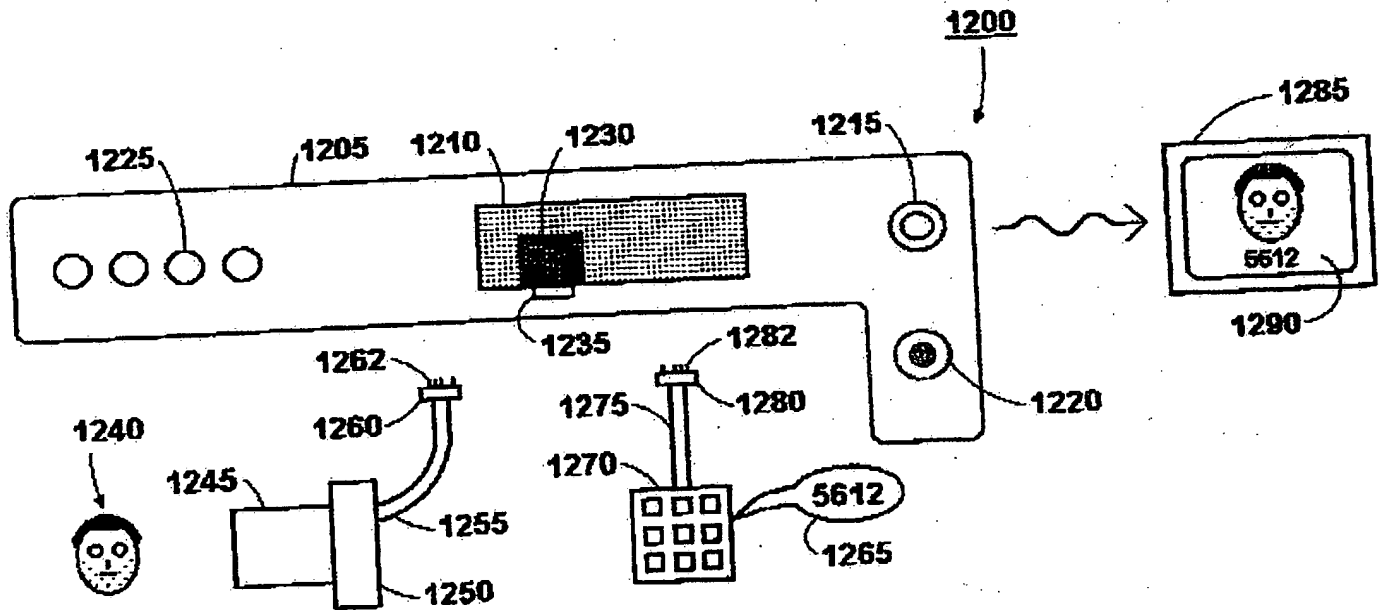


FIG. 8

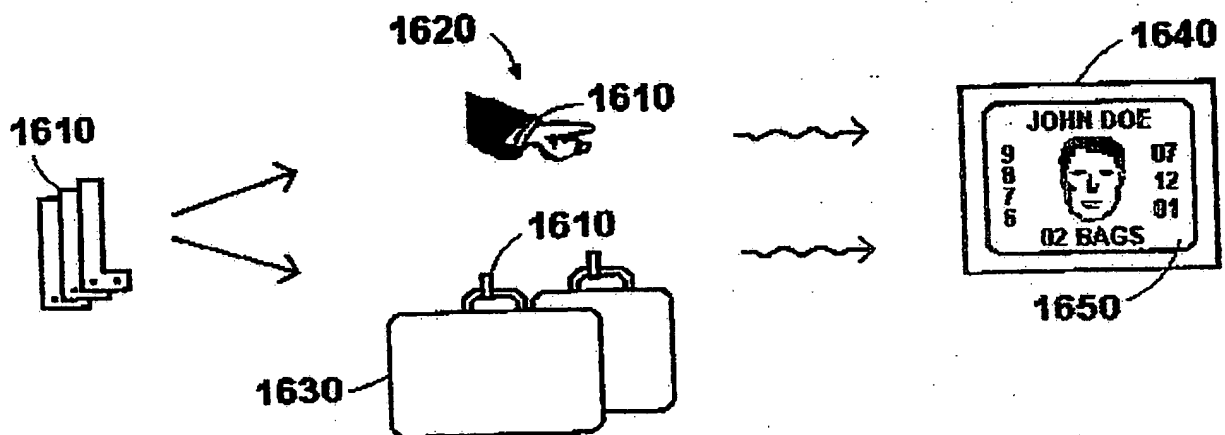
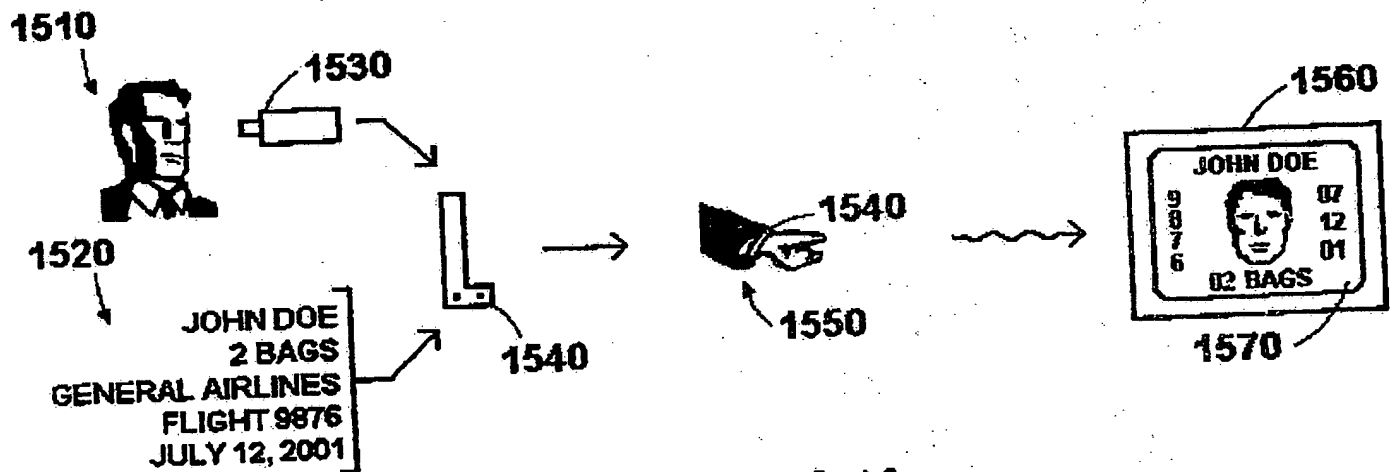
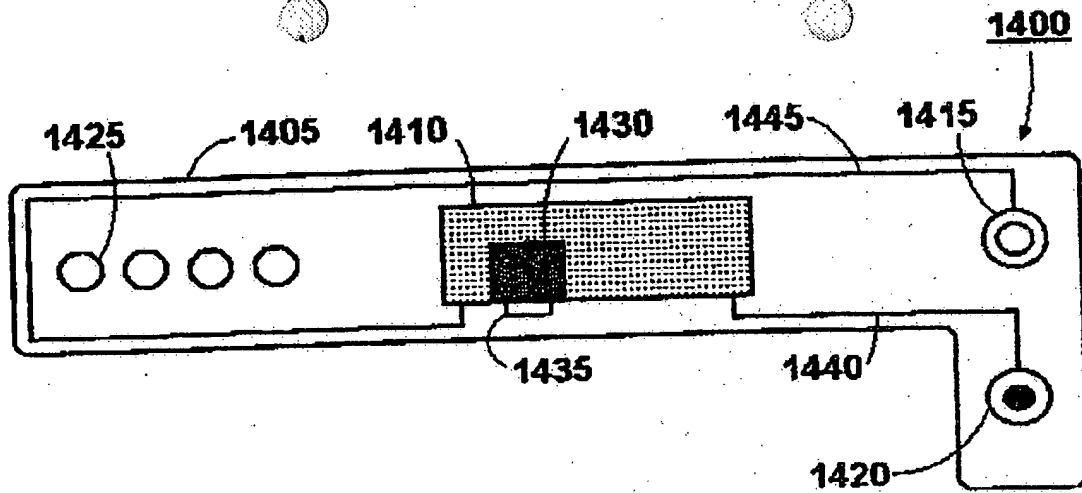


Fig 12

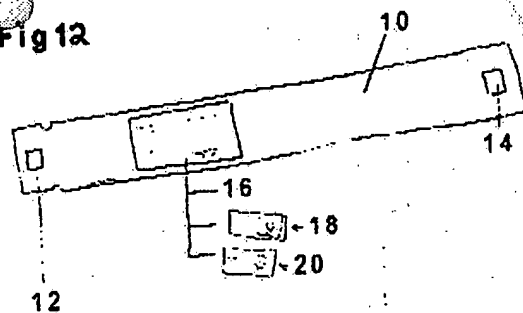


Fig 13

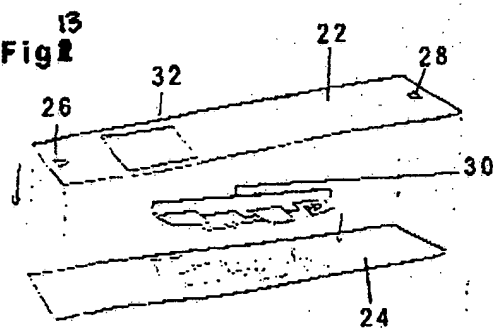


Fig 14

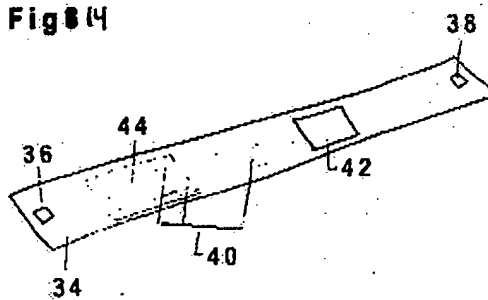


Fig 15

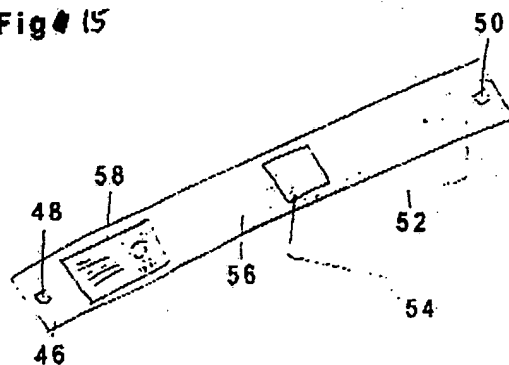


Fig 16

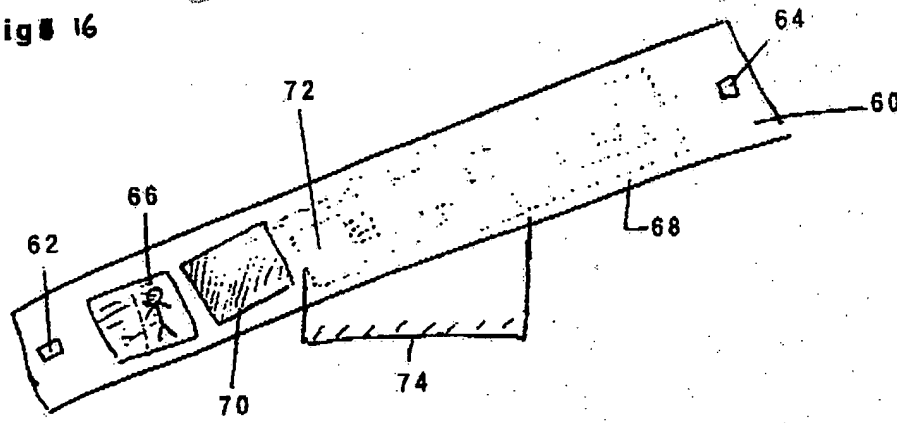


Fig 17

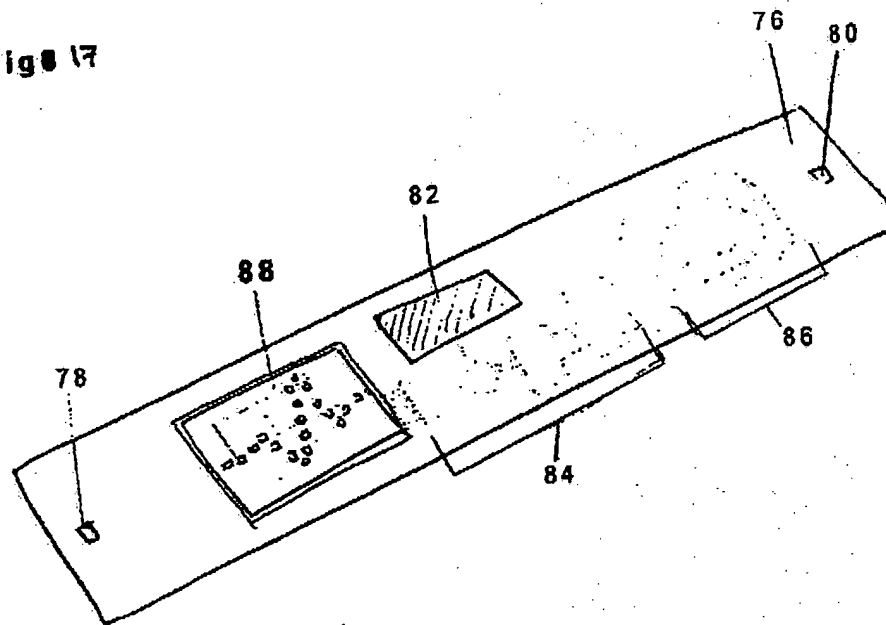
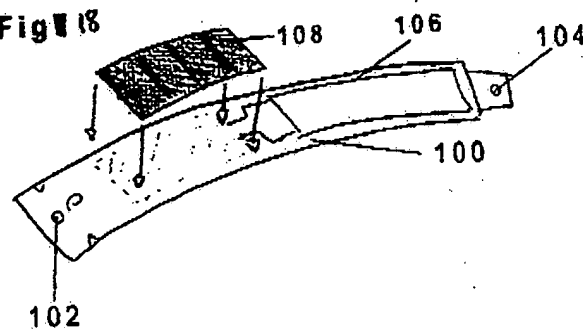


Fig 18



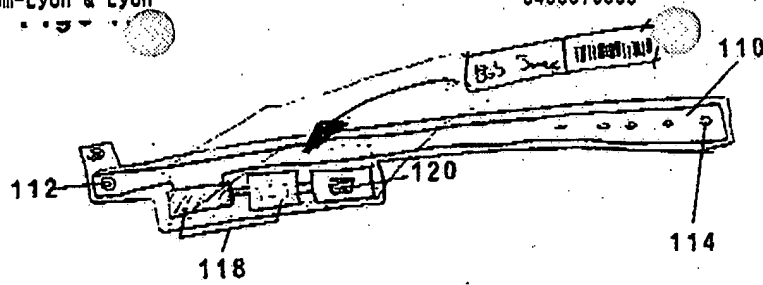


Fig 20

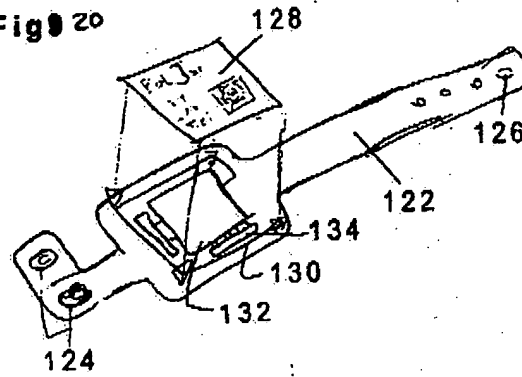


Fig 21

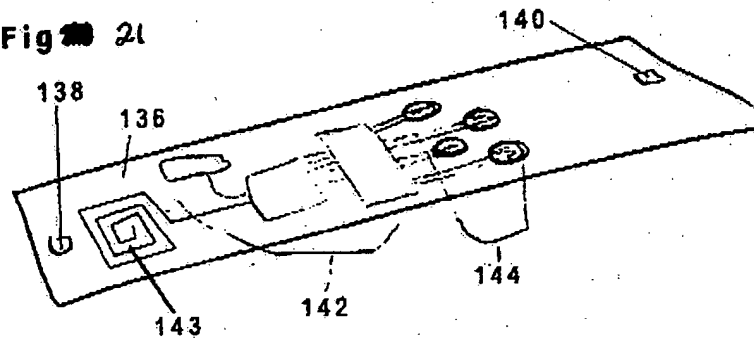


Fig 22

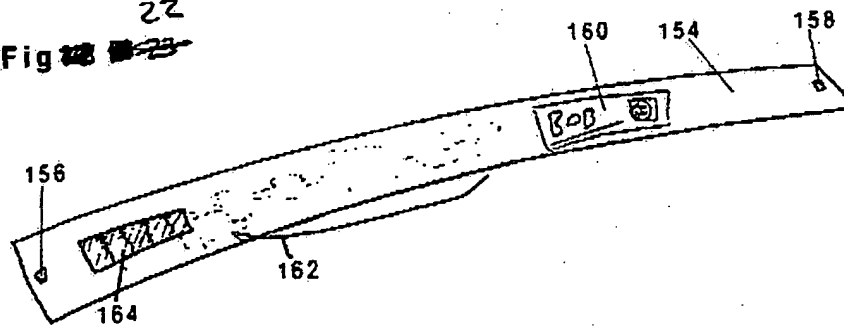


Fig 24

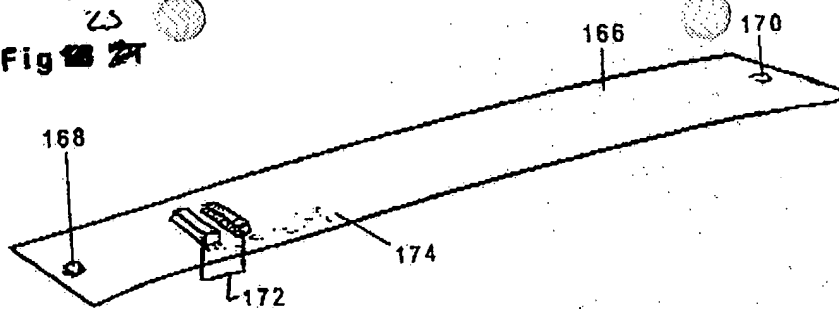


Fig 25

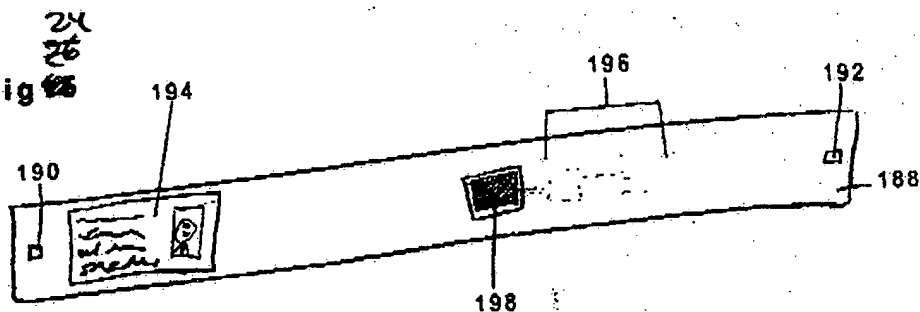


Fig 26

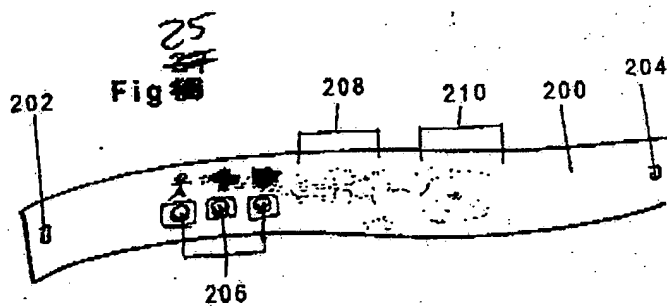


Fig 27

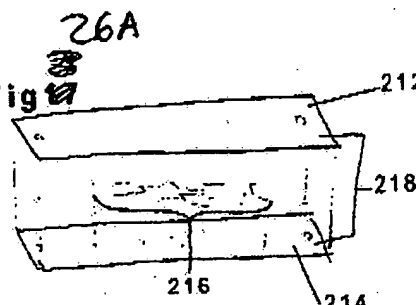
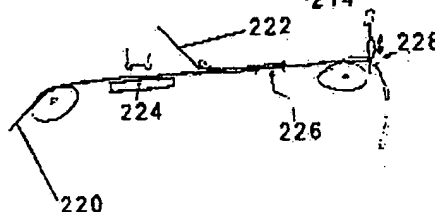
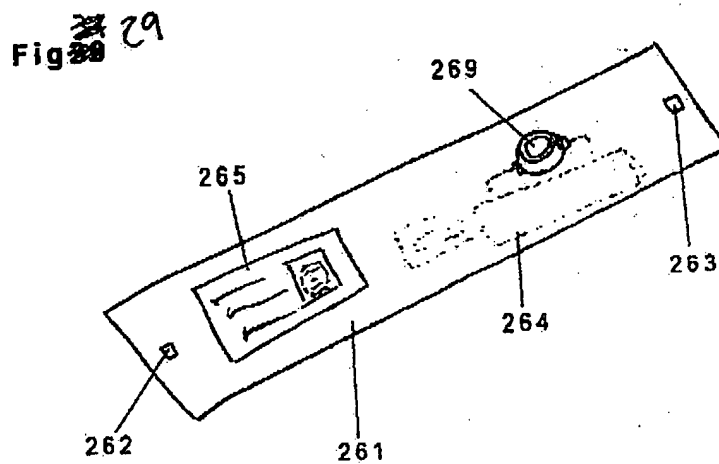
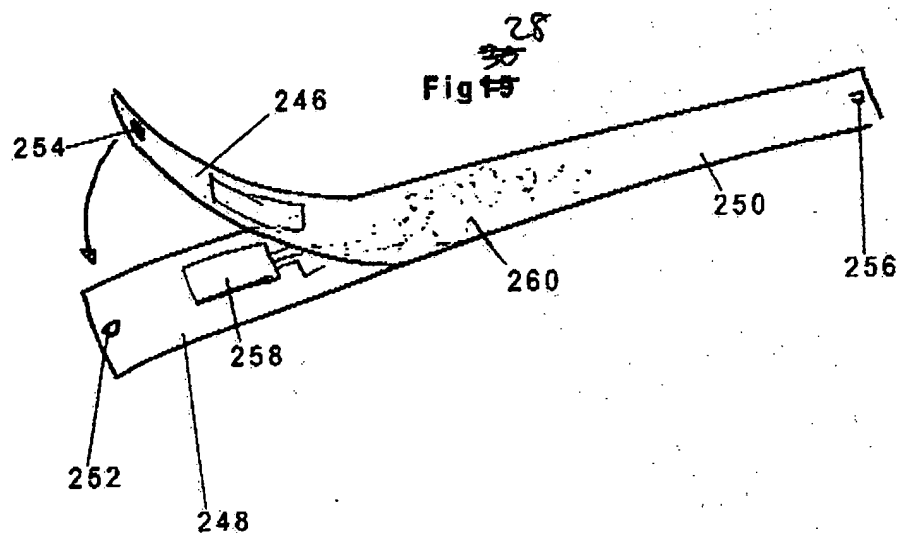
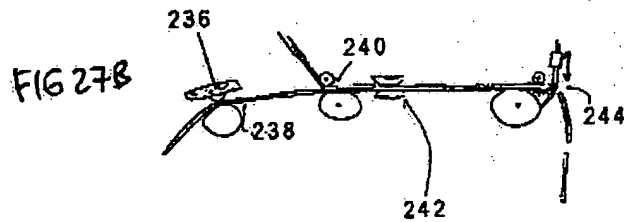
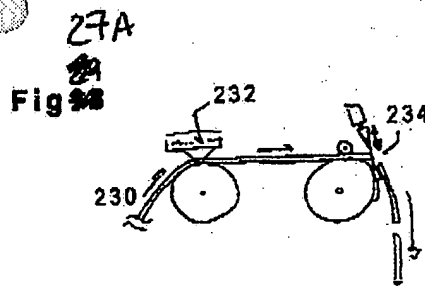
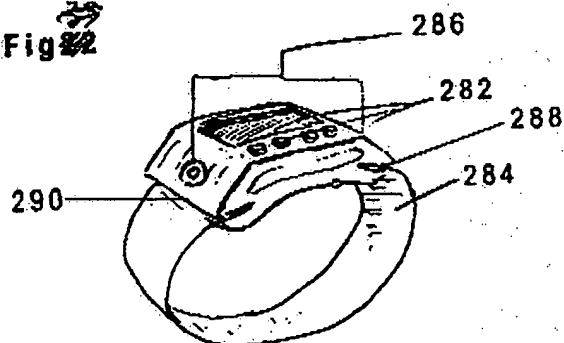


FIG 26B

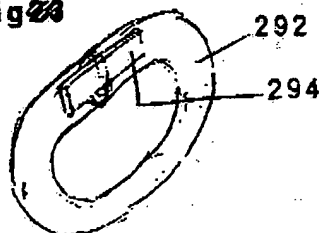




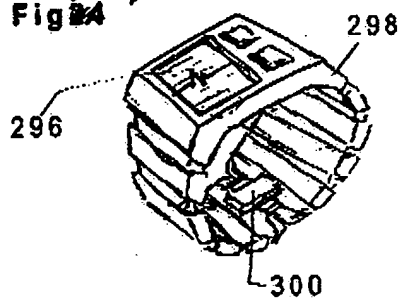
30
Fig 22

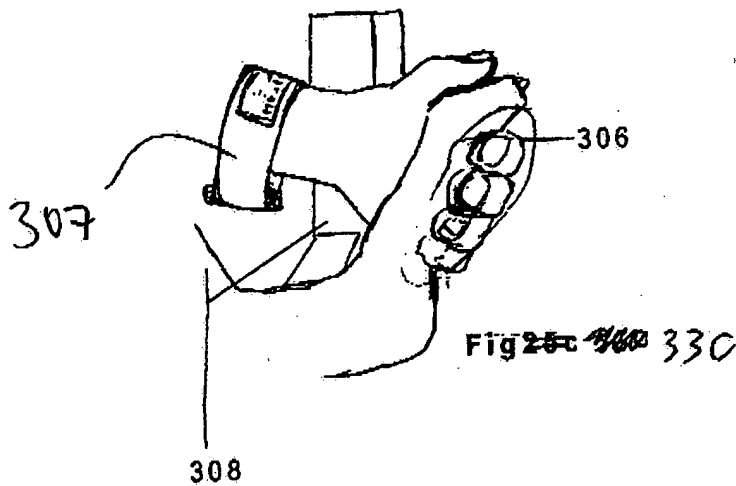
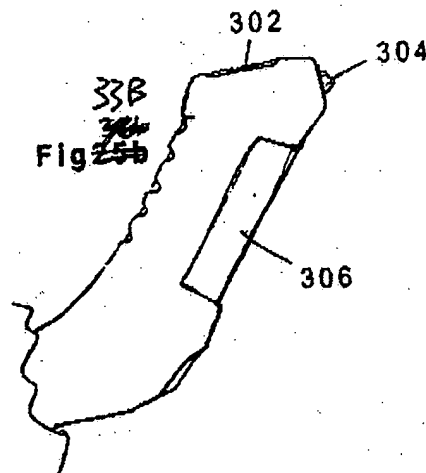
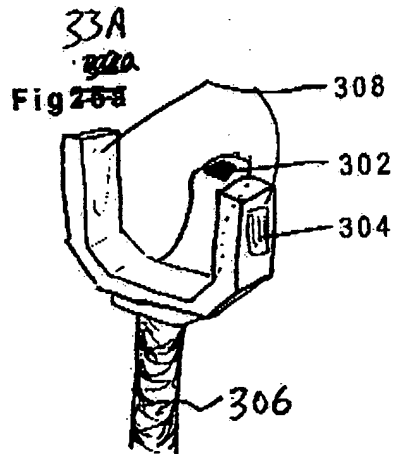


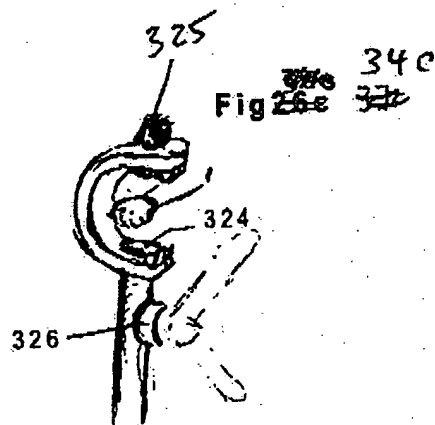
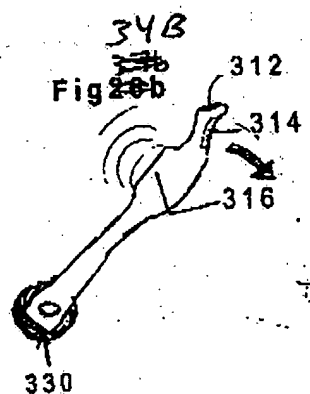
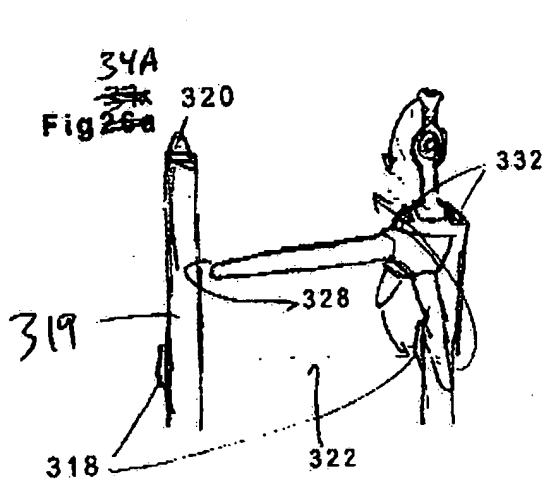
31
Fig 23

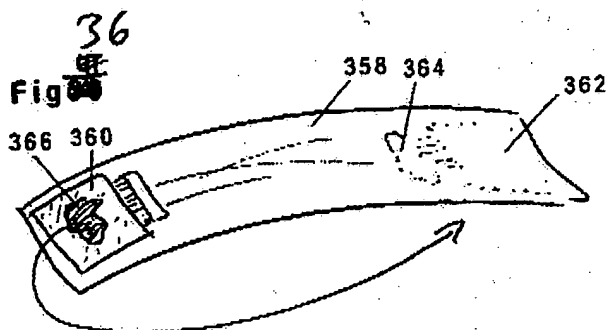
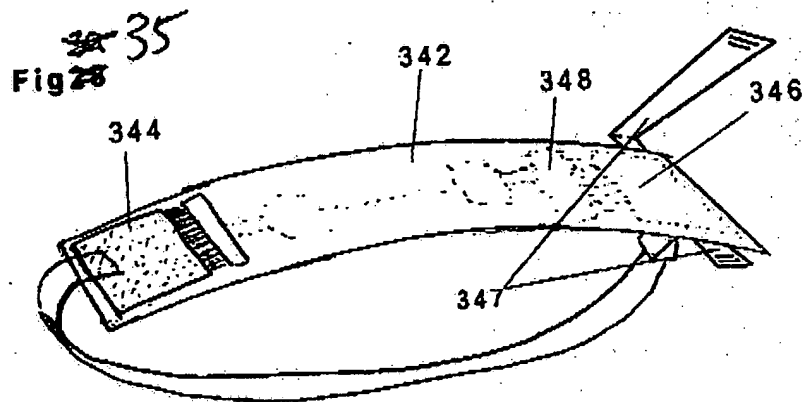


32
Fig 24









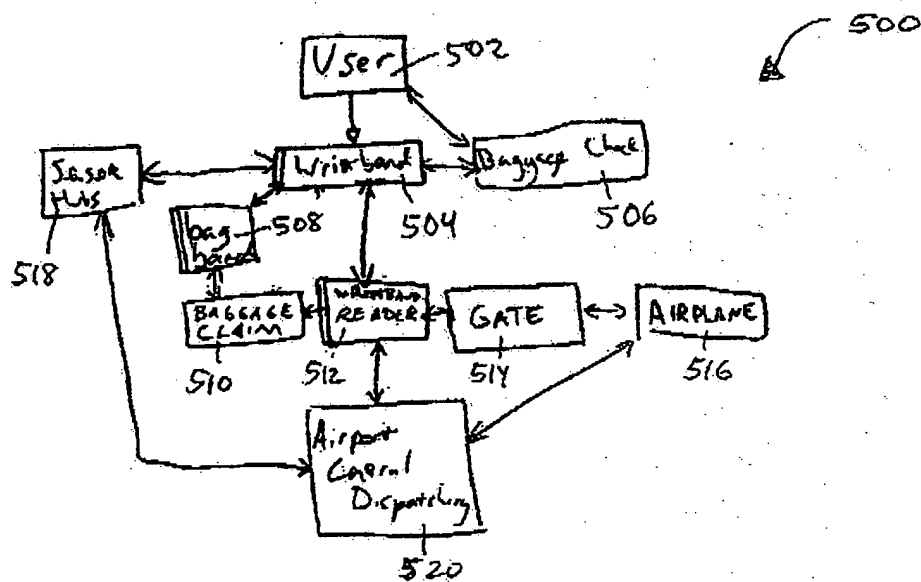


FIG. 37

500

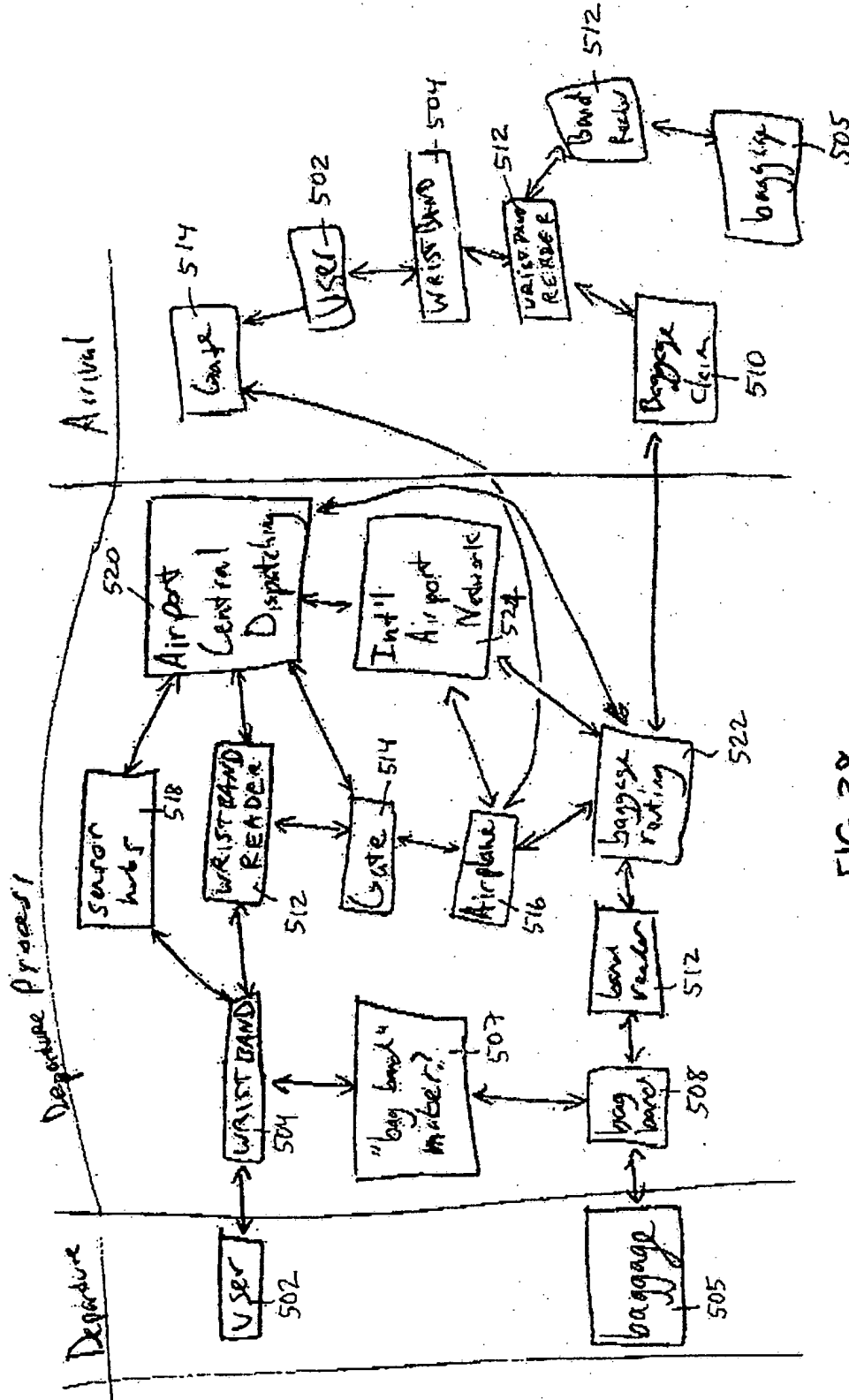


FIG. 38

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.